

Data Protection Impact Assessment on Qualtrics DesignXM

SURF Vendor Compliance

Authors: Valerija Kornilova, Julian Rill
Version: 1.0
Date: April 17th, 2026
Contact: vendorcompliance@surf.nl
DPIA by: <https://vendorcompliance.surf.nl/en>

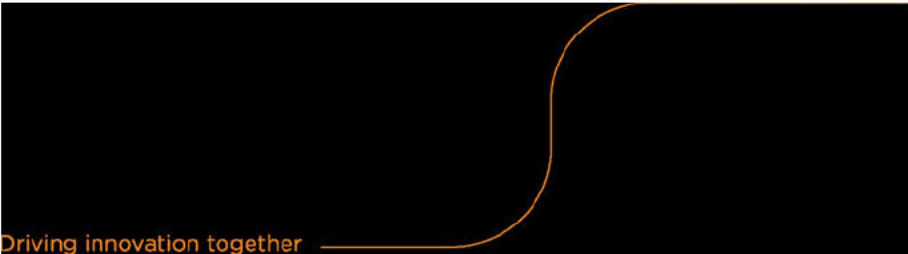
This publication is licensed under a Creative Commons
Attribution 4.0 International.

Revision History

Version	Date	Author(s)	Changes
0.1	14-07-2025	Valerija Kornilova, Julian Rill	Initial draft of part A.
0.2	31-07-2025	Valerija Kornilova, Julian Rill	Improved draft of part A.
0.3	08-10-2025	Valerija Kornilova, Jullian Rill	Improved Part A, initial draft of part B and C.
0.4	10-10-2025	Valerija Kornilova, Jullian Rill	Improved draft B and C.
0.6	26-01-2026	Valerija Kornilova, Jullian Rill	Full draft DPIA after the meeting session with Qualtrics.
0.7	30-01-2026	Valerija Kornilova, Jullian Rill	Improved full DPIA version after the internal review.
0.8	18-03-2026	Valerija Kornilova, Jullian Rill	Final DPIA before an NDA check by Qualtrics
1.0	17-04-2026	Valerija Kornilova, Jullian Rill	Final DPIA version after an NDA check by Qualtrics

Review Record

Version	Date	Reviewer(s)	Notes
0.1	16-07-2025	Sophia Gelpke, Jan Landsaat	Internal review of part A.
0.3	09-10-2025	Sophia Gelpke	Internal review of parts A,B and C.
0.6	28-01-2026	Sophia Gelpke	Internal review of the full DPIA.



Dissenting opinion provided by Qualtrics ('Oplegger')

Qualtrics' Conclusion

Qualtrics wants to emphasise that the assessments, opinions, and risk classifications contained within this DPIA are solely those of SURF. Qualtrics disagrees with many of the findings, conclusions, and classifications raised throughout this document, and has provided its feedback on the findings, conclusions and classifications to SURF. SURF ultimately decided on whether or not to incorporate this feedback into this DPIA and to publish this DPIA in its current form.

From Qualtrics' perspective, the responsibility for completing a Data Protection Impact Assessment (DPIA) rests with the Data Controller, which in this context refers to the institutions using Qualtrics services. SURF is not the data controller. Qualtrics, as the vendor providing the platform, typically does not complete DPIAs for organizations using its services. This is because the service is self-service in nature, meaning the institution determines what data to collect, from whom, and for what purposes. Since the DPIA must assess the risks specific to the controller's processing activities, and Qualtrics does not dictate these key elements, the institution is the party uniquely positioned to perform the required assessment.

Qualtrics provided SURF with information about how our services operate to assist with the completion of this DPIA. Despite repeated clarifications and objections from Qualtrics, we believe SURF have mischaracterised many elements of the DPIA, and have failed to limit this DPIA to Qualtrics' processing activities as a processor only, instead blurring the lines between where Qualtrics acts as a data controller vs. a data processor.

Additionally, Qualtrics firmly disagrees with the risk profiles that SURF has assigned to the various elements that are identified above. Qualtrics delivers services to over 20,000 customers globally and has a robust security and privacy framework designed to ensure that customers can have trust in the processing activities they conduct using our services.

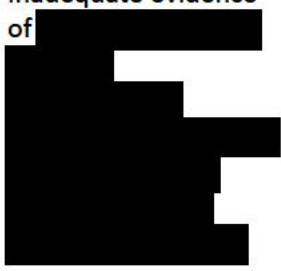
Note: The assessments, opinions, and risk classifications contained within this Data Protection Impact Assessment (DPIA) are solely those of SURF. Qualtrics disagrees with many of the findings, conclusions, and classifications raised throughout this document, and has provided its feedback on the findings, conclusions and classifications to SURF. SURF ultimately decided on whether or not to incorporate this feedback into this DPIA and to publish this DPIA in its current form.

Qualtrics' Response to individual risks

Nr.	Risk	Qualtrics response to the mitigating steps
1	Loss of control – Contractual role determination: Misalignment between legal documentation and the role of the reseller (██████████)	Qualtrics has negotiated a DPA with SURF that can be entered into directly between the education institution and Qualtrics directly.
2	Loss of Control – Data agnostic approach: Data agnostic approach allows Qualtrics not to provide specific details on data processing.	Qualtrics provides a self-service platform whereby education institutions solely determine what data to collect, from whom, and for what purposes. As such, Qualtrics cannot provide the categories of data to be processed, nor can it provide information on consent collection as education institutions are responsible for ensuring they have a legal basis for processing data. Qualtrics does not process Customer Data (as defined in its DPA) for its own purposes. All data is anonymized and aggregated before it is used by Qualtrics.
3	Inability to exercise data subjects rights – Transparency issue with the DSAR support to institutions: While survey responses are accessible, the logging information is missing.	Education institutions are the data controller when using the Qualtrics' services as they determine what data to collect, from whom, and for what purposes. As such, education institutions are responsible for responding to data subject requests. Qualtrics provides education institutions with self-service tools to enable customers to respond to data subject requests. Qualtrics does not agree with the statement that logging information should form part of the response to a DSAR. Logs are retained by Qualtrics in relation to the platform; these logs do not form part of "Customer Data" as defined in its agreements.

4	Lack of transparency in the subprocessor list – Incomplete subprocessor list: The core of this risk is the undisclosed third-party processing.	Qualtrics does not agree with the statement that the subprocessor list is incomplete. The list is available at https://www.qualtrics.com/subprocessor-list/ SURF has mistakenly identified a number of third parties as subprocessors who do not in fact act as subprocessors, therefore Qualtrics will not be adding these providers to our subprocessor list. The majority of subprocessors are optional in nature, and therefore education institutions can choose whether to leverage their services.
6	Lack of transparency reports: The risk stems from the asymmetry of information between the vendor and the public.	Qualtrics will provide this information upon request by an education institution. Qualtrics is not obligated by law to maintain a public report, and believes this is therefore unnecessary. Qualtrics has a policy to ensure that it will only comply with binding orders of governmental entities that have jurisdiction over Qualtrics or as otherwise required by law.
7	Lack of transparency – Proxy login Proxy login enables Brand Administrators to access end-user accounts without the notification.	Proxy Login is optional and fully within the control of the education institutions. Proxy logins allow Brand Admins or higher privileged accounts to log into different user accounts on the particular brand through the Users tab. By deselecting Allow Proxy Logins, no Brand Admin can directly log into a user's account. Further details about this can be found here: https://www.qualtrics.com/support/survey-platform/sp-administration/security-tab/ https://www.qualtrics.com/support/survey-platform/managing-your-account/research-core-account-settings/#GrantLoginAccess Qualtrics does not believe providing visibility to users is appropriate. Brand Admins are appointed by the education institution to manage the account on behalf of the education institution. They may be relying on proxy login for valid purposes that require that the user is not notified.

8	Loss of control - internal system and performance logs Qualtrics captures technical metrics and metadata in logs that are inaccessible to the Customer.	Qualtrics does not agree with the statement that system and performance logs are personal data. As such, Qualtrics does not agree to incorporate that information into a Data Subject Request response, or share that information incase of a Data Subject Request actioned by a customer using our self-service tools.
9	Loss of control: Reidentification of pseudonymized data – anonymisation techniques to train AI models The risk conveys the black box approach to the anonymisation techniques used by the vendor.	Qualtrics believes that its agreements are sufficient to address these concerns already. Section 3.4 of the General Terms and Conditions of Qualtrics states: <i>"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."</i> Additionally in its DPA, Qualtrics states: <i>"Qualtrics will process Personal Data only in accordance with (a) Customer Instructions or (b) Section 4.2 (Processing on Legal Requirement)."</i> The agreement template is available here: https://success.qualtrics.com/rs/542-FMF-412/images/Qualtrics%20GTC%20DPA%20%28for%20Online%29%20Template%20250523-MJR.pdf?version=0 AI Features are optional within the platform and Qualtrics enable education institutions to choose whether to use these features or not. https://www.qualtrics.com/support/xm-discover/artificial-intelligence-ai-overview-discover/
10	Loss of Control- Inadequate support for transparent user communication and informed consent Qualtrics' standard cookie banner typically lacks a 'Reject All' button on the first layer.	While Qualtrics believes that the assessment regarding cookie use has mistakenly identified cookies across multiple channels e.g. within product, Qualtrics website etc., Qualtrics will investigate the feasibility of adding a "Reject All" to its cookie consent on its marketing site. Qualtrics will investigate the feasibility of modifying the platform entry point.

11	Loss of control – Consent banner and Location information No consent banner and the collection of location information.	Qualtrics provides a self-service platform, whereby customers solely determine what data to collect, from whom and for what purposes. As such, customers are responsible for ensuring they have an appropriate legal basis for the collection and processing of any personal data. Some customers rely on consent to do this, others rely on other legal bases, e.g. legitimate interest. Qualtrics provides customers with self-service features to enable the inclusion of a consent question, notification within the survey invite etc. The recommended measure for Qualtrics here is not applicable to the customer's use of our services.
12	Inadequate evidence of 	Qualtrics makes these documents available via the Qualtrics Trust Centre: https://www.qualtrics.com/trust-center/
13	Loss of Control - Incomplete automated detection by ExpertReview of specific sensitive identifiers for Dutch education customers. The 'Sensitive data policy' feature lacks pre-configured 'topics' for Dutch-specific identifiers; it fails to fulfill its purpose for education institutions in the Netherlands.	Qualtrics "Sensitive Data Policy" is a feature, and Qualtrics does not warrant that it performs in any specific manner, or in any specific language. Qualtrics has chosen to give customers the flexibility to determine what topics to flag as sensitive. Customers have the option to create and upload their own topics using regular expressions (REGEX) so that these can be flagged, therefore we believe this option already exists. https://www.qualtrics.com/support/survey-platform/sp-administration/data-privacy-tab/compliance-assist/#SettingUp TextiQ is not applicable to the Sensitive Data Policy.

14	Lack of transparency – no publication of accuracy metrics for Sensitive Data Policy and absence of feedback mechanisms The core issue is the lack of transparency regarding performance.	Qualtrics provides information about its Sensitive Data Policy at https://www.qualtrics.com/support/survey-platform/sp-administration/data-privacy-tab/compliance-assist/ Qualtrics' "Sensitive Data Policy" is a feature, and Qualtrics does not warrant that it performs in any specific manner, or in any specific language. Qualtrics has chosen to give customers the flexibility to determine what topics to flag as sensitive. Customers have the option to upload their own topics so that these can be flagged. The "Sensitive Data Policy" feature does not rely on AI. Instead it uses customer-created REGEX expressions. Accuracy metrics cannot be produced because the policy is configured by the institution, and therefore Qualtrics does not have full context on what may be considered accurate vs. inaccurate. Accuracy will depend on whether customer-created REGEX captures every form of sensitive data that a customer is attempting to identify and whether survey respondents follow that format. If something is not identified by a customer's Sensitive Data Policy when it should have been identified, a customer can file a support ticket.
----	--	---

15	Loss of control – Automatic use of Google Translate and Amazon Translate Uncontrolled flow of data to subprocessors that are not managed directly by the institution's Brand Administrator.	Use of translation services within the platform is not automatic. Brand administrators must enable the use of third-party translation for comments in the Organization Settings tab and may also restrict the ability to translate surveys through user permissioning. Brand administrators may choose which third party its users may have access to for automatic translations and may disable third-party automatic translations altogether. Education institutions can use the services without translating materials in the platform. Education institutions also have the option to upload their own translations manually. Regardless, if education institutions choose to use the translation tools within the platform, and such translation services result in data transfers outside of the EEA, Qualtrics has implemented those measures that are required under the GDPR, including the use of EU Standard Contractual Clauses with its subprocessors, therefore all transfers are protected to an appropriate standard of data protection.
16	Transfer outside of the EU/EEA - Automatic use of Google Translate and Amazon Translate Uncontrolled flow of data to subprocessors based in the US that are not managed directly by the institution's Brand Administrator.	Please see the response to Line Item 14 above.

17	Lack of transparency and absence of consent due to the incomplete cookie information Without a complete and accurate cookie list, any consent obtained from a student or researcher is technically invalid, as they cannot be 'informed' about tracking they do not know exists.	Qualtrics disagrees that there is a lack of transparency or absence of consent. SURF have mischaracterised the use of cookies in this document, blending cookie usage on the Qualtrics website with cookie usage by institutions via use of various product features. Qualtrics does not believe that part of this assessment is applicable in the context of the DPIA as it is related to Qualtrics' role as a controller, rather than a processor. Qualtrics maintains a Cookie Policy at https://www.qualtrics.com/cookie-statement/, and allows website visitors to select their cookie preferences via the cookie banner that is presented to website visitors in Europe.
----	--	--

In the table below, there is the Qualtrics' response to the Part D of this DPIA, where SURF suggested measures for education institutions and the vendor.

Nr.	Risk	Qualtrics response to the proposed mitigation measures from Part D
1	Loss of control – Contractual role determination: Misalignment between legal documentation and the role of the reseller ('Drieam BV')	Typically, in a reseller situation, Qualtrics would expect the reseller to enter into the agreement with the end-customer, flowing down the necessary obligations. Qualtrics and SURF are finalizing the DPA between the parties.

2	Loss of Control – Data agnostic approach: Data agnostic approach allows Qualtrics not to provide specific details on data processing.	We fundamentally disagree that this is a risk. Qualtrics provides a self-service platform whereby customers (and their users) are responsible for determining what data to collect, from whom, for what purposes etc. Qualtrics does not limit the purposes of processing nor do we minimize data processes, as these are fully within the customer's control. Qualtrics has repeatedly explained that the general categories of personal data being processed is detailed in Schedule 1 of the DPA found in Exhibit A here : https://www.qualtrics.com/legal/customers/gtcs/ As detailed in the Schedule 1 of the DPA, categories of personal data are 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. As Qualtrics is data agnostic, we treat all data the same in our Cloud Service. Because Qualtrics provides a self-service platform where the Customer controls what data is collected and Qualtrics does not classify data, we would have no way of linking certain categories of personal data to specific processing purposes. Instead, Qualtrics' purpose of the processing is to provide and support the Cloud Service and any associated services as further detailed in Schedule 1 of our DPA. With respect to the services, Qualtrics only acts as a data processor, therefore any data processed by Qualtrics as a data controller is irrelevant and should not be considered a risk with respect to a DPIA. Qualtrics' processing of personal data as a controller is detailed at www.qualtrics.com/privacy-statement which clearly states the categories of personal data being processed. Qualtrics provided the following statements about the purposes of the processing: We disagree that this is a risk. We already state in section 3.5 of our terms found here:https://www.qualtrics.com/legal/customers/gtcs/ that it may create "Analyses" by using anonymized and aggregated information related to Customer's use of the Cloud Service. This already envisages that any "Customer Data" will be
---	--	--

anonymized before use. Qualtrics does not use any "Customer Data" for AI/LLM training.

The creation of Analyses is highly common in the SaaS industry. Qualtrics employs a comprehensive, multi-step process to anonymize and aggregate data before it is used for Analyses:

- Automated Removal of Identifiers: Qualtrics uses a multi-step methodology and various tools to remove personal data and brand-specific references from data sets.
- Aggregation: Data points are grouped together to further ensure anonymity while preserving analytical value.
- Human-in-the-Loop Verification: We incorporate human review into the anonymization process to validate the outcomes of automated techniques and ensure accuracy and effectiveness.
- Stringent Approval: All procedures related to data anonymization and aggregation undergo thorough internal scrutiny by appropriate stakeholders, including legal, privacy, security and engineering, and confidentiality considerations are taken into account as we design and implement our anonymization and aggregation processes.

Qualtrics' processing of personal data as a data controller is irrelevant here in our opinion. When using the Qualtrics services, the customer always acts as the data controller, and Qualtrics acts as the data processor. Our privacy policy is not applicable to Customers' use of our services and does not apply to the data they collect using the Qualtrics services.

Qualtrics provided the following information about the **categories of personal data**:

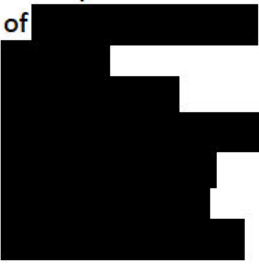
This risk seems to highlight the fundamental misalignment between the parties' roles. As the data controller, a Customer is solely responsible for determining what data to collect, from whom, for what purpose, and when to delete data when using the Cloud Service. Qualtrics acts as a data processor.

Therefore, Qualtrics cannot provide a list of every category of personal data collected as this is dependent on the customer's use. Schedule 1 of the Qualtrics DPA clearly details that the categories of personal data are determined by the customer acting as the data controller. Schedule 1 of the Qualtrics DPA also states 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. As detailed above in D.1.2 - As Qualtrics is data agnostic, we treat all data the same in our Cloud Service. Because Qualtrics provides a self-service platform where the Customer controls what data is collected and Qualtrics does not classify data, we would have no way of linking certain categories of personal data to specific processing purposes. Instead, Qualtrics' purpose of the processing is to provide and support the Cloud Service and any associated services as further detailed in Schedule 1 of our DPA.
3	Inability to exercise data subjects rights – Transparency issue with the DSAR support to institutions: While survey responses are accessible, the logging information is missing.	Qualtrics fundamentally disagrees that our DSAR tools are lacking. We are clear in their capabilities here. We provide self-service tools to enable customers to action data subject requests. If the automated tools do not include specific data, Qualtrics enables customers to action deletions or other requests via other means, with assistance from Qualtrics as needed to comply with applicable laws. Qualtrics maintains detailed system and performance logs (which include IP addresses, protocols, and requests), but these full logs are internal only and unavailable to Customers. No response data is captured in log files. A subset of our internal logs are made available to Customers in the platform as an activity log - https://www.qualtrics.com/support/survey-platform/sp-administration/security-tab/, or via API - https://api.qualtrics.com/a3fb9b11bbf0e-public-api-enterprise-audit-service-api-spec). The purpose of collecting this information is to prevent and protect against fraud and malicious activity, and to ensure the security of the website, app or cloud service of Qualtrics.
4	Lack of transparency in the subprocessor list – Incomplete subprocessor list: The core of this risk is the undisclosed third-party processing.	Again, Qualtrics fundamentally disagrees with this characterisation. Qualtrics list of subprocessors can be found here: https://www.qualtrics.com/subprocessor-list/. We notify customers when we appoint new subprocessors. As is standard for cloud service providers, we engage subprocessors across all of our customers, so we cannot permit an individual customer to have a consent right over any individual subprocessor. Instead customers have the right to object to new subprocessors and terminate as described in the DPA.

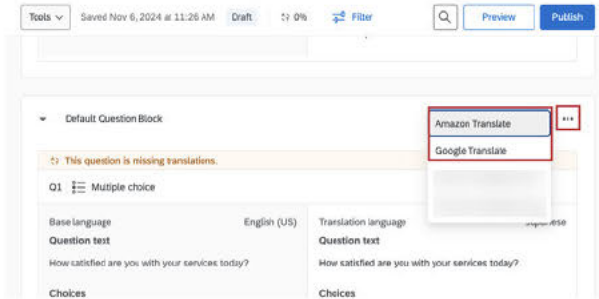
		Within the platform, customers can control whether to use optional technical subprocessors. This is detailed in our support documentation.
6	Lack of transparency reports: The risk stems from the asymmetry of information between the vendor and the public.	We do not intend to maintain an online transparency report, but disagree this is a risk. We provide information about the number of requests received upon customer request. Can you please advise why this is a risk if the customer will receive the information upon request? Additionally, as detailed in the DPIA, Qualtrics will only comply with binding orders of governmental entities that have jurisdiction over Qualtrics or as otherwise required by law. In such cases, Qualtrics will (i) give Customer reasonable written notice to allow Customer to seek a protective order or other appropriate remedy (except to the extent that compliance with the foregoing would cause Qualtrics to violate a court order or other legal requirement), (ii) disclose only such information as is required by the governmental entity or otherwise required by law, and (iii) use commercially reasonable efforts to obtain confidential treatment for any confidential information so disclosed.
7	Lack of transparency – Proxy login Proxy login enables Brand Administrators to access end-user accounts without the notification.	

8	Loss of control - internal system and performance logs Qualtrics captures technical metrics and metadata in logs that are inaccessible to the Customer.	Performance logs are not part of the DPA because they do not contain personal data. Can you please advise as to why the logs should be disclosed given they do not contain personal data? Qualtrics' logging activities are legally permissible in accordance with our agreements. Qualtrics maintains detailed system and performance logs (which include IP addresses, protocols, and requests), but these full logs are internal only and unavailable to Customers. No response data is captured in log files. A subset of our internal logs are made available to Customers in the platform as an activity log - https://www.qualtrics.com/support/survey-platform/sp-administration/security-tab/ , or via API - https://api.qualtrics.com/a3fb9b11bbf0e-public-api-enterprise-audit-service-api-spec). The purpose of collecting this information is to prevent and protect against fraud and malicious activity, and to ensure the security of the website, app or cloud service of Qualtrics.
9	Loss of control: Reidentification of pseudonymized data – anonymisation techniques to train AI models The risk conveys the black box approach to the anonymisation techniques used by the vendor.	Qualtrics does not publish its anonymization process publicly as this is proprietary information. We disagree that this is a risk as we believe this is an industry-standard approach. Qualtrics' contractual obligations are clear about our obligations and we do not process Customer Data to train any AI model. We anonymize and aggregate Customer Data prior to model training. Our process incorporates Human-in-the-Loop Verification to validate the effectiveness of the automated removal of personal data. We use proprietary rules and machine learning techniques combined with human intervention and oversight to identify and remove personal data and brand-specific references. The human review step specifically exists to ensure the accuracy and effectiveness of the anonymized data and to validate the outcomes of automated techniques before the data is aggregated. Qualtrics also continues to publish information related to our AI processes in our Trust Centre. Please confirm if SURF have already reviewed these documents.

10	Loss of Control- Inadequate support for transparent user communication and informed consent Qualtrics' standard cookie banner typically lacks a 'Reject All' button on the first layer.	While we disagree that this is a risk, even if it is a risk, it is not a risk related to the Qualtrics services we provide to customers. The Qualtrics cookie banner and statement are not applicable to the customer's use of the services. Qualtrics' cookie banner is about individuals visiting the Qualtrics website at www.qualtrics.com. Qualtrics manages consent on that website via a third party, OneTrust. While the language "Reject All Cookies" is not available, website visitors can control the cookies being used via the "Manage Cookie Preferences" option. We would like to request further details about the testing performed by SURF and the process followed as we do not believe the website operates as described, but we are happy to investigate further. Cookie use should be controlled by the user, via our third party system, One Trust.
11	Loss of control – Consent banner and Location information No consent banner and the collection of location information.	As stated above, the MetaInfo question does not collect IP or geo-location information. This information was included in the survey response because the survey was set up to collect IP address, but this can be disabled within the Survey Options tab. Qualtrics also offers a Consent Form option as detailed here: https://www.qualtrics.com/support/survey-platform/common-use-cases-rc/building-a-consent-form/ Because Qualtrics does not determine the legal bases on which the customer relies to process personal data, we do not propose an out-of-the-box consent question as this will need to be tailored to the customer's requirements.
12	Inadequate evidence of 	Qualtrics' new SOC2 report is available within the Qualtrics Trust Centre.

13	Loss of Control - Incomplete automated detection by ExpertReview of specific sensitive identifiers for Dutch education customers. The 'Sensitive data policy' feature lacks pre-configured 'topics' for Dutch-specific identifiers; it fails to fulfill its purpose for education institutions in the Netherlands.	This is not a risk, it is a product feature request. Qualtrics "Sensitive Data Policy" is a feature, and we do not warrant that it performs in any specific manner, or in any specific language. Qualtrics has chosen to give customers the flexibility to determine what topics to flag as sensitive. Customers have the option to upload their own topics so that these can be flagged, therefore we believe this option already exists. https://www.qualtrics.com/support/survey-platform/sp-administration/data-privacy-tab/compliance-assist/#SettingUp Qualtrics is data agnostic, we do not treat "sensitive data" with a "higher level of protection." Instead, we protect all data the same way in our Cloud Service. So while a Customer (or their Permitted Controllers) will solely determine whether any "Special Categories of Personal Data" are collected via the Cloud Service, this will not change how we process Customer Data therefore no risks exist. Qualtrics has taken Technical and Organizational Measures as described in the DPA to ensure a level of security appropriate to protect also Special Categories of Personal Data.
----	---	--

14	Lack of transparency – no publication of accuracy metrics for Sensitive Data Policy and absence of feedback mechanisms The core issue is the lack of transparency regarding performance.	Qualtrics offers multiple options to customers to provide feedback about our services. For general feedback or support, customers can submit a request through the Qualtrics Customer Success Hub. Additionally customers can submit product ideas here. For the end customers, depending on license size, customers may be assigned a Technical Success Manager who regularly meets with the customer to discuss their XM program, overall goals, and product requests. Can we clarify if SURF reviewed these options before identifying this as a risk?
----	--	--

15	Loss of control – Automatic use of Google Translate and Amazon Translate Uncontrolled flow of data to subprocessors that are not managed directly by the institution's Brand Administrator.	This is not accurate. The Qualtrics automatic translation feature uses third-party services but this is highlighted within the platform.  The text of the survey questions is sent to the third-party and will be returned in the language the customer selects. This feature only sends your survey text if you choose to translate your surveys. However, these are optional services. As detailed in our subprocessor list found here: https://www.qualtrics.com/subprocessor-list/, these services are used as optional subprocessors, not mandatory subprocessors. Therefore, these vendors will only be engaged if the customer requests to use these services offered by Google and Amazon. Customers also have the option of uploading translations thereby negating the need to use the third-party services within the platform. Further details can be found here: https://www.qualtrics.com/support/survey-platform/survey-module/survey-tools/translate-survey/
16	Transfer outside of the EU/EEA - Automatic use of Google Translate and Amazon Translate Uncontrolled flow of data to subprocessors based in the US that are not managed directly by the institution's Brand Administrator.	Please see the response to Line Item 14 above.

17	Lack of transparency and absence of consent due to the incomplete cookie information Without a complete and accurate cookie list, any consent obtained from a student or researcher is technically invalid, as they cannot be 'informed' about tracking they do not know exists.	As above, we believe our website is already operating so that users have full control over the cookies that are used in the "Manage Cookie Preferences" option. Can you provide further details about the testing so we can investigate why you might have been seeing cookies in the manner you described. We're more than happy to provide further responses on this topic as we learn more.
----	--	---

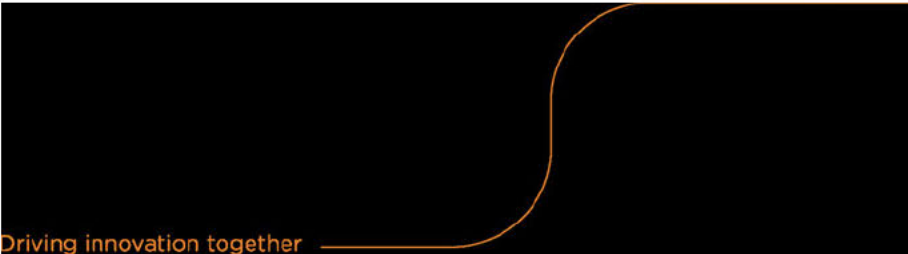
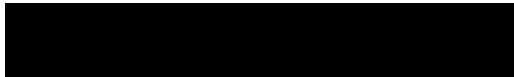
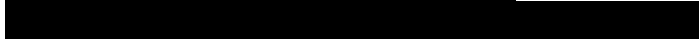


Table of Contents

Dissenting opinion provided by Qualtrics ('Oplegger')	4
List of Tables and Figures	25
Glossary of Terms.....	26
Summary	27
The scope of this DPIA.....	27
Introduction	34
The scope of this DPIA.....	36
Methodology	37
Outline of this DPIA	39
Part A Description of Data Processing.....	40
A.1 Description of Services	40
A.2 Contractual Framework.....	43
A.3 Data Processing Purposes	51
A.4 Processed Personal Data	54
A.5 Data Processing Activities	64
A.6 Processing Techniques and Methods.....	75
A.7 Cookie Statement.....	93
A.8 Involved Parties	99
A.9 Interests in Data Processing	101
A.10 Processing Locations	103
A.11 Legal and Policy Framework.....	105
A.12 Retention Periods.....	108
Part B Assessment of Lawfulness of Data Processing	110
B.1 Legal Basis	110
B.2 Special Categories of Data and Sensitive Data	120
B.3 Purpose Limitation	121
B.4 Necessity and Proportionality	122
B.5 Data Subject Rights	127
Part C Description and Assessment of Risks to Data Subjects	129
C.1 Introduction	129
C.2 Risks to Data Subjects	130
Part D Description of Proposed Mitigation Measures	142

D.1	Mitigation Measures	142
Appendix 1 Technical Testing Scenarios		154
1.1	Testing Software and Hardware.....	154
1.2	Qualtrics Accounts	154
1.3	Scenario 1: Login and Authentication	156
1.4	Scenario 2: Creating Qualtrics Projects	157
1.5	Scenario 3: Designing Surveys.....	158
1.6	Scenario 4: Configuring Survey Options	160
1.7	Scenario 5: Distributing Surveys to Participants	161
1.8	Scenario 6: Anonymously Answering Surveys.....	162
1.9	Scenario 7: Survey Answering via Targeted Links	163
1.10	Scenario 8: Data Analysis on Survey Results	164
Appendix 2 User Type Role Permissions		165
1.11	General.....	165
1.12	Survey Platform.....	175
1.13	Employee Experience	179
1.14	Website Feedback	180
1.15	Contacts	181
Appendix 3 Mapped Endpoints.....		182

List of Tables and Figures

Table 1 HORA business processes fulfilled with Qualtrics	52
Table 2 Qualtrics' data processing purposes.....	53
Table 3 Qualtrics' DPA details of processing	56
Table 4 Privacy Statement categories of personal data (Qualtrics as a controller).	57
Table 5 Personal data mapping for Qualtrics as a processor	59
Table 6 Question Types available within Qualtrics	61
Table 7 Strictly Necessary Cookies for Qualtrics	94
Table 8 Functional Cookies for Qualtrics.....	94
Table 9 Performance Cookies for Qualtrics.....	95
Table 10 Social Media Cookies for Qualtrics	95
Table 11 Targeting Cookies for Qualtrics	96
Table 12 Mandatory Subprocessors.....	101
Table 13 Data backups	109
Table 14 Accounts used during technical testing within Qualtrics	155
Figure 1 Collected data from Meta Info Question Type.....	62
Figure 2 Anonymise responses option within survey settings	62
Figure 3 Survey setting saving respondent's survey data, enabled by default	67
Figure 4 Standard disclaimer on survey provided by Qualtrics (circled in red).....	67
Figure 7 Column renaming while translating	81
Figure 8 Qualtrics warning for using Google Translate	81
Figure 9 Enabling or disabling translation services (Google Translate, Amazon Translate).....	81
Figure 10 Prompt to discover backbone of the AI Response Task	83
	84
	85
Figure 5 Sensitive Data Policy Set-up	89
Figure 6 Configuring topics for Sensitive Data Policy	90
Figure 13 Qualtrics Cookie Consent Banner within SURF's Qualtrics testing environment	93
Figure 14 Risk Matrix.....	130

Glossary of Terms

Term	Abbreviation	Definition
Data Protection Impact Assessment	DPIA	Describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible.
Data Transfer Impact Assessment	DTIA	Assesses the risks that may arise when transferring personal data from one country to another, particularly outside the EU/EEA, if such third countries do not have an adequate decision.
SURF Vendor Compliance	SVC	The internal team where this plan takes part of. Undertakes compliance assessments on vendors where industry demand exists for in-depth discussions around privacy and security.
Dutch research and education organisations	Education organisations	This plan is written for the Dutch research and education organisations, sometimes abbreviated to “the Dutch education sector” or “education organisations”.
Data Protection Authority	DPA	An independent public body responsible for upholding information rights and ensuring compliance with data protection laws.
Data Processing Agreement	DPA	This is a legally binding contract that outlines how personal data will be handled between two or more parties, specifically a data controller and data processor.
Data controller	Controller	It is an entity which determines the purposes for which and the means by which personal data is processed.
Data processor	Processor	The processing is to be carried out on behalf of a controller; the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
Subprocessor	N/A	This is a third-party entity that a data processor engages to help process personal data on behalf of a data controller.

Summary

This document is a DPIA (Data Protection Impact Assessment) on Qualtrics DesignXM. This DPIA is commissioned by SURF, the collaborative organisation for IT in Dutch higher education and research, sometimes abbreviated to 'The Dutch education sector' or 'education institutions'. This DPIA is a reference DPIA which means that the findings may be used for the SURF members and education sector.

Qualtrics services

Qualtrics XM enables organisations to collect real-time feedback from students, faculty, and staff through channels such as surveys, online reviews, call center interactions, and social media. This feedback offers insights into community experiences and concerns, supporting initiatives to enhance student engagement and improve staff retention in a rapidly evolving academic landscape.

The scope of this DPIA

This DPIA looks at Qualtrics DesignXM system. Within offered services to the education institutions (SURF members), SURF determined the scope based on the questionnaire which was shared with our educational institutions in February of 2025.

As the result of the questionnaire shared with SURF members, SURF found out the purpose of Qualtrics' digital services which is mainly for the scientific research in education (application of teaching methods), research (data collection, data processing and analysis) and knowledge exploitation (knowledge marketing).¹ In the subsequent research, SURF aimed to precisely define the scope of institutional activities. It was determined that Qualtrics DesignXM falls within the domain of Experience Management (XM).² This service can be used to enhance how education institutions operate and improve overall student and staff experiences. It offers tools for administrators, general users, and researchers to manage surveys, collect data, and perform analysis.

General User & Researcher Capabilities:

- Project creation using templates or custom surveys
- Advanced survey logic and validation features
- Survey quality checks via ExpertReview
- Collaboration features with customisable permissions
- Multiple distribution methods and response tracking
- Basic analysis tools and export options (SPSS, Excel, etc.)
- Quota setting for representative sampling
- Translation support with auto/manual options
- Access to training, documentation, and support through XM Basecamp and the Qualtrics Community

Administrator Capabilities (Brand Admins):

¹ Results of the Qualtrics Questionnaire shared with member institutions on the 15th February.

² Qualtrics, 'Education Experience Management' (no date) <https://www.qualtrics.com/education/> accessed 17 March 2026.

- Full control over licenses, user creation, and permission settings
- Management of data privacy policies (e.g., sensitive data detection, security settings)
- Oversight of platform usage (response rates, active users)

This DPIA will further explain the purpose of Qualtrics DesignXM as a digital service for the institutions, which features it offers through the explanation of services, personal data processed, processing activities, and the responses of the DSARs (data subject access requests).

Out of scope

This DPIA excludes the services such as Qualtrics CoreXM and Qualtrics AI response. SURF conducts testing within the environment of Qualtrics DesignXM.

Outcome of the DPIA

This DPIA identified 14 high and 1 low risks associated with the use of Qualtrics Design XM for Education. The mitigating measures proposed in Part D by SURF, education institutions may view the measures that SURF suggested to mitigate some of the risks. These measures correspond to low risks and features that may be disabled by the institutions. The high risks are unlikely to be resolved without firm and concrete commitments from Qualtrics to implement appropriate technical and organisational measures at the vendor level.

The high risks identified concern the following: the data agnostic approach, incomplete list of subprocessors, loss of control and transparency due to the incomplete consent collection, incomplete cookie lists and incomplete handling of the DSARs. Mitigating measures for the education institutions are found in Part D Description of Proposed Mitigation Measures. The vendor has not committed to implementing mitigating measures and has disputed the SURF's risk classification. Qualtrics shared the dissenting opinion in the form of 'Oplegger' with SURF which is included in the section Dissenting opinion provided by Qualtrics ('Oplegger') **Qualtrics'**

Conclusion

SURF's objective is to ensure that the use of Qualtrics' products by education customers within the Netherlands is fully compliant with the GDPR. As SURF is at the forefront of conducting and publishing DPIA outcomes of behalf of its members. Given the unresolved high risks identified, SURF urges education institutions to carefully consider the findings of this DPIA before continuing using Qualtrics' platform.

Should Qualtrics provide firm commitments to implement the necessary mitigating measures, SURF will update this assessment accordingly.

The table below presents the overview of the remaining 14 high risks and 1 low risk.

Nr.	Risk	Measures to be taken by institutions	Measures to be taken by Qualtrics advised by SURF
1	Loss of control – Contractual role determination: Misalignment between legal documentation and the role of the reseller [REDACTED]	Explicitly state in the DPA that data breach notifications shall be directed to the vendor from the education institutions. SURF proposes to sign a direct DPA with Qualtrics. If a direct DPA is not plausible or possible, add an addendum to the current agreement that Qualtrics is the sole processor. [REDACTED] should be stated as a 'reseller' or 'commercial intermediary'.	
2	Loss of Control – Data agnostic approach: undermining the parties' role allocation and purpose limitation principle.	Since the vendor will not provide categories, the institution must implement strict 'data records' for end-users such as researchers, staff or student. By limiting what fields can be created in the platform, the institution can 'self-document' the categories of data and data subjects. Ensure that only the 'informed' core processing occurs. Prohibit the use of the platform for special categories of data. Education institutions should have an explicit 'No-AI/LLM training based on the processing of Customer's data'. Ensure that education institution's own privacy notice explicitly lists the categories of personal data that vendor processes as a data processor and, possibly, as a data controller. In the Schedule 1, the categories of personal data should be mapped to the purposes.	Modular public page which includes specific information about the usual data categories processed and the mapped purposes to the personal data. Clearly distinguish which data is processed by Qualtrics as a data controller and/or data processor. Negotiate and provide education institutions an explicit 'No-AI/LLM training based on the processing of Customer's data' in the DPA. Commit contractually to the absolute anonymisation (not just pseudonymization) for any data used for 'Research and development' or 'Product improvement'. Give education institutions an option to opt out from the anonymisation processes. Map the categories of personal data which Qualtrics processes in accordance with 7 purposes for which

			Qualtrics acts as a data controller Publish a public Data mapping for all Qualtrics products that list every possible category of personal data collected. Provide a transparency dashboard for the admin to observe what exactly categories are being used, for example, for service development.
3	Inability to exercise data subjects rights – Transparency issue with the DSAR support to institutions: While survey responses are accessible, the logging information is missing.	When the DSAR misses certain categories of data, establish a formal procedure within the institution which includes sending a manual ticket to Qualtrics support specifically requesting the missing data. Introduce the manual to the end-users about an updated DSAR tool.	Qualtrics should add the missing logging information and submit the full DSAR response to education institutions.
4	Lack of transparency in the subprocessor list – Incomplete subprocessor list: The core of this risk is the undisclosed third-party processing.	Request the information from the vendor about the full subprocessor list, and do it periodically within an education institution. Disable the features associated with the third-party processing until the vendor adds a clear description of their purpose.	Add the mentioned subprocessors to the list of subprocessors. Provide opt-out which allows institutions to disable all third-party telemetry for the end-users.
5	Lack of transparency reports: The risk stems from the asymmetry of information between the vendor and the public.	While the specific Qualtrics report may be confidential, the institution can include a high-level statement in its own public transparency report. For example: <i>'Our vendors have reported zero data disclosure requests from foreign intelligence authorities in the previous calendar year.'</i>	Launch a web page that provides aggregated, anonymized statistics on government requests globally. This should include: Number of requests received; Percentage of requests challenged or rejected; Categories of data requested.

6	Lack of transparency – Proxy login Proxy login enables Brand Administrators to access end-user accounts without the notification.	Disable proxy login	Implement real-time end-user notification. For example, it should be visible not only for the admin, but for the users who are being masqueraded on. Role-based limitations: restrict what an impersonator can access during a session.
7	Loss of control - internal system and performance logs Qualtrics captures technical metrics and metadata in logs that are inaccessible to the Customer.	Explicitly mention in the DPA that performance logs are part of the data category in Schedule 1 of the DPA.	Publish a list for Customers that lists exactly what metadata is captured in performance logs. Provide the full copy of personal data (including the complete DSAR).
8	Loss of control: Reidentification of pseudonymized data – anonymisation techniques to train AI models The risk conveys the black box approach to the anonymisation techniques used by the vendor.	Insert a strict clause into the DPA stating that anonymisation and aggregation of institutional data for AI training or product improvement are strictly prohibited. Formally request a report on the metrics for Dutch-language. If the vendor cannot provide these, the institution should assume the anonymisation is technically insufficient. Use the Brand Administrator settings to globally disable all generative AI features and automated insights until the vendor provides a transparency whitepaper that includes a list of all data fields being scrubbed.	Qualtrics should publish a list of the data types its ML model is trained to detect. Qualtrics should be more transparent about Dutch performance statistics. Explain and show the percentage/metrics of AI-anonymized data that is manually reviewed by human auditors. Be more transparent about Dutch performance statistics, explain thresholds and metrics for the human in the loop.
9	Loss of Control- Inadequate support for transparent user communication and informed consent	Build a dedicated consent form. Instruct researchers to add these consent forms and put it in if meta info is used (amongst any other	Update the global platform theme to include a 'Reject All' button as a standard feature, rather than requiring custom code from the Customer.

	Qualtrics' standard cookie banner typically lacks a 'Reject All' button on the first layer.	questions that might reveal personal data).	Re-engineer the platform's entry point so that no non-essential cookies (analytics, functional preferences) are dropped until the consent API receives a positive signal from the user.
10	Loss of control – Consent banner and Location information No consent banner and the collection of location information.	Build a dedicated consent form. Instruct researchers to build consent forms and inform the researchers about the processing of location data being processed (amongst any other questions that might reveal personal data).	Design the measure so non-essential cookies (analytics, functional preferences) are dropped until the consent API receives a positive signal from the user.
12	Loss of Control - Incomplete automated detection by ExpertReview of specific sensitive identifiers for Dutch education customers The 'Sensitive data policy' feature lacks pre-configured 'topics' for Dutch-specific identifiers, it fails to fulfill its purpose for institutions in the Netherlands.	Set the 'Sensitive data policy' to redact sensitive information from survey responses. This ensures that even if a respondent unprompted enters their BSN in an open-text field, the data is replaced with asterisks or other substitute. Do not actively configure personal data through the ExpertReview	Improve the Text iQ and ExpertReview to understand Dutch labels for sensitive data. For example, recognizing BSN will trigger for sensitive data warnings.
13	Lack of transparency – no publication of accuracy metrics for Sensitive Data Policy and absence of feedback mechanisms The core issue is the lack of transparency regarding performance.	File tickets or support requests to Qualtrics for the feedback.	Qualtrics should participate in quarterly reviews to discuss known detection gaps and provide a roadmap for improving Dutch-specific identification together with SURF. Add a 'flag as inaccurate' button directly for the Sensitive Data Policy.
14	Loss of control – Automatic use of Google Translate and Amazon Translate Uncontrolled flow of data to	A manual action for the user who translates need to do (i.e. append 'AI translated to EN') to the field.	Qualtrics will provide a build-in feature for the institution to manually use the translate services.

	subprocessors that are not managed directly by the institution's Brand Administrator.		
15	Transfer outside of the EU/EEA - Automatic use of Google Translate and Amazon Translate Uncontrolled flow of data to subprocessors based in the US that are not managed directly by the institution's Brand Administrator.	Inform the end-users about the translation functionality.	Provide other option for translation: European alternatives. Provide an option for the brand administrators to add additional translation options manually.
16	Lack of transparency and absence of consent due to the incomplete cookie information Without a complete and accurate cookie list, any consent obtained from a student or researcher is technically invalid, as they cannot be 'informed' about tracking they do not know exists.	Issue a formal instruction to the vendor to deactivate any cookies identified as 'Marketing' or 'Targeting' that are not strictly necessary for the service.	Qualtrics should provide a real-time, machine-readable list of all cookies currently in use. This would allow educational institutions to automatically update their own transparency notices whenever the vendor adds a new tracker. For every cookie used, Qualtrics must provide a clear technical justification proving it is 'Strictly necessary' under Article 5(3) of the ePrivacy Directive.

Introduction

Qualtrics DesignXM provides an experience management platform enabling organisations to develop custom surveys and research studies which are tailored to specific educational objectives. This Data Protection Impact Assessment (DPIA), commissioned by SURF (the Dutch IT cooperative of education and research) examines the personal data processing that occurs when Qualtrics is used by Dutch higher-education and research institutions.

About SURF

SURF is the collaborative organisation for IT in Dutch education and research, owned by its member universities and research institutes. Through SURF, members jointly procure high-quality digital services, develop and share knowledge, and ensure compliance with data protection regulations. As part of its services, SURF conducts umbrella DPIAs for IT services widely used across the sector.

What is a DPIA?

DPIA stands for Data Protection Impact Assessment and must be performed by data controllers when they process personal data in a way that may “result in a high risk to the rights and freedoms of natural persons”, according to article 35 of the General Data Protection Regulation (GDPR). The assessment is intended to shed light on, among other things, the specific processing activities, the inherent risk to data subjects, and the safeguards applied to mitigate these risks. The purpose of a DPIA is to ensure that any risks attached to the process in question are mapped and assessed, and that adequate safeguards have been implemented to mitigate those risks.

Data subjects have a fundamental right to protection of their personal data and some other fundamental freedoms that can be affected by the processing of personal data, such as freedom of expression. The right to data protection is therefore broader than the right to privacy. Consideration 4 of the GDPR explains:

“This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.”

Umbrella DPIAs versus individual DPIAs

In GDPR terms, SURF is not the data controller for the processing of personal data via the use of Qualtrics’ products and services. The data controller is the individual educational or research institutions that uses this service. However, as the Dutch IT cooperative, SURF takes the responsibility to assess the data protection risks for the end users and to ensure the data processing complies with the GDPR. Therefore, SURF conducts umbrella DPIAs to assist its members to select a privacy-compliant deployment, and conduct their own DPIAs where necessary. Only the organisations themselves can assess the specific data protection risks, related to the technical privacy settings, nature and volume of the personal data they process and vulnerability of the data subjects. The Dutch DPA has endorsed this approach to improve the

protection of personal data within the Education sector.³ This umbrella DPIA is meant to help educational and research organisations with the DPIA they must conduct when they deploy Qualtrics, but it cannot replace the specific risk assessments the organisations must make themselves.

Performing one umbrella DPIA on an IT service has benefits for SURF's members, as well as for the vendors of the products SURF assesses. For the members, it saves the cost of each of them having to do an entire DPIA individually. They are also able to incorporate their combined knowledge about a product and experiences with a vendor in the umbrella DPIA. Additionally, SURF can more effectively negotiate mitigating measures with the vendors, because it has the combined negotiating power of the entire sector as a representative. For the vendors, it saves time, effort and money as well to not have to assist every institution individually with DPIAs that will likely be very similar. It's also more efficient for them to be able to implement measures that benefit all members at once.

DPIA criteria

The Dutch Data Protection Authority (Dutch DPA) has published a list of seventeen types of processing for which a DPIA is always mandatory in the Netherlands.⁴ If a processing is not included in this list, an organisation must itself assess whether the data processing is likely to present a high risk. The European national supervisory authorities (hereinafter referred to as the Data Protection Authorities or DPAs), united in the European Data Protection Board (EDPB) have also published a list of nine criteria. As a rule of thumb, if a data processing meets two of these criteria a DPIA is required.

The circumstances of the data processing via Qualtrics DesignXM ('Design XM') meet three out of nine criteria from the EDPB's list.⁵ This criteria is overall applicable to the education institutions.

1. Sensitive data or data of a highly personal nature (criterion 4). The EDPB explains: *"some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected)."* For example, later in Part A, SURF will mention that Qualtrics processes sensitive information such as bsn (burgerservicenummer).

This criterion is relevant when education institutions conduct research or administrative activities involving questionnaires, surveys, or academic studies that collect information on special categories of personal data such as health information, political opinions, religious or philosophical beliefs, etc. These fall under the GDPR's 'special categories of personal data'.

³ Dutch DPA (in Dutch only), Sectorbeeld Onderwijs 2021-2023, 24 January 2024, p. 5-6, URL:

[https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023](https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023;);

https://www.edpb.europa.eu/sme-data-protection-guide/be-compliant_en

⁴ https://www.edpb.europa.eu/our-work-tools/consistency-findings/register-decisions/2019/netherlands-sas-list-kind-processing_en

⁵ Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, page 9.

2. Data processed on a large scale (criteria 5). Working Party 29 recommends that the following factors should be considered when determining large scale processing:
 - a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population. Large-scale data and the ability to organise large scale surveys.⁶
 - b. the volume of data and/or the range of different data items being processed;
 - c. the duration, or permanence, of the data processing activity. The processing of personal data varies from normal categories of data to special categories of data.
 - d. the geographical extent of the processing activity. Since both the USA and Europe are in the geographical scope.
3. Matching or combining datasets (criterion 6): two or more data processing operations performed for different purposes in a way that would exceed the reasonable expectations of the data subject (against the principle of purpose limitation mentioned in Article 5 GDPR). This is due to the discovered purposes during SURF technical research that Qualtrics processes personal data to train its AI models.
4. The processing involves data relating to vulnerable data subjects (criterion 7). Employees and students whose personal data are processed via Qualtrics DesignXM are in a position of unequal power relative to the educational and research institutions overseeing the processing activities. Furthermore, the surveys may elicit the input of special categories of personal data by end-users. As such, heightened attention to data protection obligations and ethical considerations is required in these contexts.

Qualtrics stated that the categorisation applicable to this scenario is not exhaustive because the processing activities are determined by education institutions.⁷ Hence, education institutions should consider if additional circumstances are applicable.

The scope of this DPIA

This DPIA looks at Qualtrics DesignXM system. Qualtrics XM for enables organisations collect real-time feedback from students, faculty, and staff through channels such as surveys, online reviews, call center interactions, and social media. This feedback offers insights into community experiences and concerns, supporting initiatives to enhance student engagement and improve staff retention in a rapidly evolving academic landscape.

Within offered services to the education institutions (SURF members), SURF determined the scope based on the questionnaire which was shared with our educational institutions in February of 2025. In this questionnaire, SURF asked which Qualtrics products and features they use and what business processes they fulfil with the product. In addition, the scope was further refined by having meetings with the representatives of the institutions that use Qualtrics to discuss their process of using Qualtrics in day-to-day activities. The results that institutions presented was that the purpose of Qualtrics' digital services was mainly for the scientific research in education (application of teaching methods), research (data collection, data processing and analysis) and knowledge exploitation (knowledge marketing).⁸

⁶ <https://community.qualtrics.com/survey-platform-54/large-scale-survey-1500-questions-28769?tid=28769&fid=54>

⁷ Qualtrics feedback to the DPIA v0.7 from the 20th of February 2026.

⁸ Results of the Qualtrics Questionnaire shared with member institutions on the 15th February.

In the subsequent research, SURF aimed to precisely define the scope of institutional activities. It was determined that Qualtrics DesignXM falls within the domain of Experience Management (XM).⁹ This service can be used to enhance how education institutions operate and improve overall student and staff experiences. It offers tools for administrators, general users, and researchers to manage surveys, collect data, and perform analysis.

General User & Researcher Capabilities:

- Project creation using templates or custom surveys
- Advanced survey logic and validation features
- Survey quality checks via ExpertReview
- Collaboration features with customisable permissions
- Multiple distribution methods and response tracking
- Basic analysis tools and export options (SPSS, Excel, etc.)
- Quota setting for representative sampling
- Translation support with auto/manual options
- Access to training, documentation, and support through XM Basecamp and the Qualtrics Community

Administrator Capabilities (Brand Admins):

- Full control over licenses, user creation, and permission settings
- Management of data privacy policies (e.g., sensitive data detection, security settings)
- Oversight of platform usage (response rates, active users)

This DPIA will further explain the purpose of Qualtrics DesignXM as a digital service for the institutions, which features it offers through the explanation of services, personal data processed, processing activities, and the responses of the DSARs (data subject access requests).

Out of scope

This DPIA excludes the services such as Qualtrics CoreXM and Qualtrics AI response.

Methodology

This DPIA was developed through a multi-faceted approach combining desk research, technical research, and structured engagement with Qualtrics. The aim was to evaluate both the legal and technical dimensions of personal data processing by institutions using the Qualtrics services.

Desk Research formed the foundation of the legal and policy analysis. This involved systematically reviewing documentation provided by Qualtrics, including data processing agreements, privacy policies, internal procedures, and relevant information security certifications. These documents were assessed against GDPR obligations, with particular attention to the legal basis for processing, data subject rights, international transfers, and roles of the parties involved. In cases where ambiguities or gaps in documentation were identified, SURF issued targeted follow-up questions to Qualtrics. Their responses were incorporated into our findings, and their opportunity to clarify positions contributed to the accuracy and fairness

⁹ Qualtrics, 'Education Experience Management' (no date) <https://www.qualtrics.com/education/> accessed 17 March 2026.

of the assessment. The outcomes of this documentation review are integrated throughout the DPIA.

Technical Research focused on understanding the data lifecycle within Qualtrics from a systems and architecture perspective. This included evaluating how data is collected, processed, stored, shared, and secured. The investigation drew upon available technical documentation and system design descriptions, alongside real-world and live testing of the system, and interactive discussions with Qualtrics. Specific areas of analysis included data flows, storage methods, system logs, privacy-related settings, and the application of security controls. These findings were then cross-referenced with the legal review to assess alignment between stated policies and technical implementation, and to identify any areas of residual risk or non-compliance. The testing scenarios were carried out by SURF in the environment provided by the vendor.

The DPIA used a grey box methodology. This allowed SURF to maintain an independent, external perspective while also engaging in focused, informed access to specific parts of the systems. It offered a pragmatic balance. It's sufficiently thorough to examine high-risk areas in depth, yet not so demanding as to resemble a full system inspection. In practical terms, we started with an external analysis based on observable behaviours and available documentation, then followed up by verifying key findings through direct communication with Qualtrics.

The cooperation process was complex and differed from other vendor engagements. For the significant part of the project, the communication was conducted through a single person from Qualtrics – there was no direct involvement of legal or technical teams in the beginning of the SURF DPIA research. The importance of the DPIA for the Dutch education sector was communicated to the vendor throughout the DPIA process. Despite SURF's requests for deeper insight into internal data processing, the lack of technical insights prevented the intended 'grey box' approach for the research. When the identified risks were presented to the vendor, Qualtrics acknowledged the significance of this DPIA and the broader implications for its education customers in the Netherlands, particularly given that this report is made publicly available.

Qualtrics explained this cooperation approach:

*'Qualtrics does not perform DPIAs on behalf of customers. We provided the necessary documentation to enable SURF to complete the DPIA. This documentation is the documentation we provide to all customers. As institutions determine what data to collect and for what purposes, Qualtrics cannot opine on significant portions of the DPIA. That being said, Qualtrics is providing more thorough responses to this DPIA because you are considering publishing this document and we believe it categorically contains inaccurate information and misrepresentations.'*¹⁰

Recognising the effect of this DPIA on education institutions, the publicity of this assessment after SURF re-emphasised the importance of this DPIA, Qualtrics eventually became more forthcoming. During a final meeting to fill in the gaps of the first report, Qualtrics provided more

¹⁰ Qualtrics' feedback to the SURF DPIA version 0.7 from the 20th of February 2026.

granular information and more internal process details the vendor had previously been reluctant to share, allowing SURF to address the issues.

Outline of this DPIA

This DPIA is based on the structure of the Model Gegevensbeschermingseffectbeoordeling Rijksdienst (DPIA), and on the structure developed by SURF Vendor Compliance team. This combination helps to implement the technical investigation results with legal analysis.

This DPIA uses a structure of four main divisions, which are reflected here as “parts”.

- A. Description of the factual data processing
- B. Assessment of the lawfulness of the data processing
- C. Assessment of the risks for data subjects
- D. Description of mitigation measures

Part A explains the processing activities using Qualtrics in detail in general terms, based on the tested setup.¹¹ This part describes the services within the scope of this DPIA, we will look at the purposes of the data processing from the perspective of the vendor as controller and processor, analyse project documentation such as privacy statements, security and privacy certifications. For this part, project documentation has been reviewed, as well as the contracts with Qualtrics. In addition, test scenarios were executed, and a data subject access request was submitted.

Part B provides an assessment by SURF of the lawfulness of these data processing activities through Qualtrics. This analysis starts with an analysis of the extent of the applicability of the GDPR and the ePrivacy Directive, in relation to the legal qualification of the role of Qualtrics as provider. Subsequently, SURF has assessed conformity with the key principles of data processing, including transparency, data minimisation, purpose limitation, and the legal ground for the processing, as well as the necessity and proportionality of the processing.

Part C assesses the risks to the rights and freedoms of the data subjects created by the processing activities identified in Qualtrics in Part A of this DPIA. It names specific risks that derive from these processing activities and aims to specifically determine both the likelihood that these risks may occur, and the severity of the impact on the rights and freedoms of the data subjects if the risks occur.

Finally, **Part D** contains concrete measures that can be taken by Qualtrics and the educational institutions to mitigate the risks identified in Part C. These measures might either reduce the chance of the risks to occur, or the impact they might have, or both. Part D also contains an assessment of any residual risk attached to the use of Qualtrics that could not be mitigated by applying the suggested measures. If such unmitigated risks remain, the educational institution implementing Qualtrics might be required to consult the supervisory authority prior to the processing.

¹¹ Find the test scenarios in Appendix 1.

Part A Description of Data Processing

Part A of this DPIA provides an overview of the relevant facts of the data processing operations. It describes the data processing operations, the processing purposes and the interests in the data processing operations. In addition, Part A provides an overview of the personal data processed, the parties involved, and the techniques and methods of data processing. Also covered are the legal and policy framework and retention periods.

A.1 Description of Services

This section outlines the architecture of Qualtrics Design XM ('Qualtrics'), detailing its system design, core components, data flows, and the technologies that ensure its scalability, security, and performance. SURF will explain the rationale behind selecting Qualtrics DesignXM for the DPIA and detail the platform's core features and capabilities.

A.1.1 Qualtrics as a vendor

Qualtrics is a US based experience management company headquartered in Provo, Utah. It specialises in experience management (XM). This software enables organisations to collect, analyse, and transform the feedback (raw feedback) into the observable results. In the European Union ('EU'), Qualtrics' EMEA headquarters office is located in Ireland.

A.1.2 Qualtrics XM for Education

Before diving into the licenses offered by Qualtrics CoreXM and Qualtrics DesignXM, SURF will firstly identify which services Qualtrics offers to the institutions.

*'Experience management (XM) is the process of listening closely to feedback, understanding what your stakeholders are saying, and then taking action to create the experiences they want.'*¹²

Qualtrics XM for Education is a platform designed for schools and universities to gather real-time feedback from students, faculty, and staff across various sources such as surveys, online reviews, call centre interactions, and social media. The usage of the tooling involves the collection of personal data. This is the list of popular cases for Educational institutions to use Qualtrics XM:¹³

- Student feedback;
- Course evaluations where support may be needed;
- 360 employee engagement;
- Alumni and donor feedback;
- Event and program evaluations;
- Research and data collection.

A.1.3 Qualtrics Core XM

Based on the output of the questionnaire shared with SURF's member, Qualtrics CoreXM is the basic package that education institutions use.

Stemming from the questionnaire, Qualtrics CoreXM is the foundational platform of Qualtrics' Experience Management (XM) Suite, designed to help organisations gather, analyse, and act on

¹² Qualtrics, *Education Experience Management* (Qualtrics, accessed 10 March 2026) <https://www.qualtrics.com/education/>.

¹³ Qualtrics, *Education Experience Management* (Qualtrics, accessed 30 July 2025) <https://www.qualtrics.com/education/>.

experience data across four key areas: Customer, Employee, Product, and Brand. It provides a flexible, scalable, and secure system for measuring and improving experiences at every touchpoint.¹⁴

Even though Qualtrics Core XM is used by the majority of education institutions in the Netherlands, it has similar features to the DesignXM which is an enhanced digital service. Although few institutions use it, conducting a DPIA on DesignXM offers a clearer understanding about the features. Qualtrics Design XM is explained in the next section.

Before diving more into the differences between the services that Qualtrics offers to education institutions, it should be noted that the term ‘customer’, used in the Sections below about Core XM and Design XM, refers to the institution rather than an individual user.

A.1.4 Qualtrics Design XM

Qualtrics Design XM is a premium component of the Qualtrics Experience Management (XM) platform that empowers organisations to intentionally create and refine experiences based on data-driven insights.¹⁵ Design XM emphasizes proactive experience creation by using research, modelling, and testing tools to shape customer, employee, product, and brand experiences even before they are fully deployed. Design XM is an extension of Core XM, and is more expensive license in comparison to Core XM.

A.1.5 Overview of Architecture

Qualtrics operates as a self-service, cloud-hosted, multi-tenant SaaS platform. This means that the underlying infrastructure and its operational maintenance are managed by Qualtrics, while customers are responsible for their day-to-day programme management and functionality usage. The cloud service is hosted on Amazon Web Services (AWS).

Customers have the option to select their preferred data centre region from the available choices. For instance, Dutch educational institution could opt for a primary location in Frankfurt, Germany, with a replication fall-over location in Dublin, Ireland. This DPIA assumes education organisations select EU-based data centres to store their data.

Qualtrics explained that Dutch education institutions as per customer determine the location of data centre.¹⁶

Qualtrics uses a hot standby (active/passive) configuration. This design ensures geographic resilience using at least two AWS availability zones within the chosen region. In a disaster recovery scenario, services can be recommenced in a geographically resilient site to restore the cloud service. Each data centre is engineered for high availability, thereby eliminating single points of failure, including redundant communication lines and power supplies.

¹⁴ Qualtrics CoreXM Ranked #1 in Survey Platform in G2 Fall 2022 Report (Qualtrics, 28 September 2022) <https://www.qualtrics.com/articles/news/g2-fall-report-2022/> accessed 29 January 2026.

¹⁵ Qualtrics, *Meet our powerful experience design tool – DesignXM* (Qualtrics, 8 July 2021) <https://www.qualtrics.com/articles/news/experience-design-tool-designxm/> accessed 29 January 2026.

¹⁶ Qualtrics feedback from the 20th of February 2026.

Within the Qualtrics data centre environment, direct access is protected by internal hardware firewalls and Intrusion Detection and Prevention Systems (IDS and IPS). Load balancers distribute traffic across web and application servers to enhance reliability and performance. These application servers are designed to scale rapidly to meet demand, sending processed data to database servers for long-term storage. Wireless networks within Qualtrics' corporate environment are encrypted with WPA2 and require Multi-Factor Authentication (MFA).

A.1.6 Educational institutions' order forms

In this chapter, SURF will describe the Qualtrics order form.¹⁷ This Order form is a standard document that specifies the details of a transaction between Qualtrics and Customers (education institutions). The Cloud Services purchased by the Education Institutions are specified in the applicable order form. the following:

CoreXM Use-case;

CoreXM Users;

CoreXM Responses;

CoreXM Additional Responses.

Order forms mention CoreXM, which is used predominantly in the Dutch educational sector. From the survey responses of our education institutions, SURF determined that in addition to CoreXM, DesignXM is used by our members. Since CoreXM is the foundational platform for collecting and analyzing experience data, DesignXM is an expanded version of CoreXM providing advanced features for designing and optimizing customer and product experience as stated by Qualtrics.¹⁸ Therefore, the scope of this DPIA is the analysis of the DesignXM since it is an extended version of the CoreXM. CoreXM is outside the scope of this DPIA.

Additionally, the Order form is based on the Agreement that Qualtrics and Educational institutions conclude. Data Processing Agreement will be discussed later in this DPIA.

It is important to mention that the Order Form is subject to the Qualtrics' General Terms and Conditions.¹⁹ Order Form does not only mention the services purchased, but also the list of special categories of personal data as referenced in the Schedule 1 of the DPA.²⁰

The reasoning that Qualtrics provided for including the special categories of personal data in the Order Form is:

'The primary reasons for listing the intent to collect Special Categories of Personal Data in the Order Form (OF) rather than fixing them definitively in the DPA are to ensure accuracy, future-proof the agreement, and reflect the customer's sole responsibility as the controller.'

¹⁷ Qualtrics Order Form 006VH00000Pums2YAD (the number of the order form).

¹⁸ Qualtrics, *Meet our powerful experience design tool – DesignXM* (Qualtrics, 8 July 2021) <https://www.qualtrics.com/articles/news/experience-design-tool-designxm/> accessed 29 January 2026.

¹⁹ Qualtrics Order Form 006VH00000Pums2YAD (the number of the order form).

²⁰ Qualtrics, *'General Terms and Conditions for Indirect Qualtrics Services (GTC) and Data Processing Agreement (DPA) (for Online) Template'* (23 May 2025) <https://success.qualtrics.com/rs/542-FMF-412/images/Qualtrics%20GTC%20DPA%20%28for%20Online%29%20Template%20250523-MJR.pdf> accessed 17 March 2026.

*The DPA is intended to be used across all future orders and for the duration of the agreement between the parties. If the Special Categories of Personal Data were exhaustively listed in the DPA, any change in the Customer's data collection practices (e.g., beginning to collect health data when they previously did not) would require amending the DPA itself. By referencing the Order Form, the parties can document the current intention regarding sensitive data collection without undermining the long-term validity of the core DPA.*²¹

From Qualtrics' perspective, this approach provides better accuracy and allows the Customer to use the services as a self-service platform:

*'Therefore, while the Customer (Controller) is solely responsible for its privacy notice and processing register, the documentation provided via the DPA's Schedule 1 and the Order Form assists the Customer in fulfilling these obligations by clearly identifying the scope of potential high-risk data being processed on the platform.'*²²

A.2 Contractual Framework

This section will outline legal documentation between Qualtrics and education organisations. We will further analyse general legal documents such as Qualtrics' Master Terms and Conditions, General Terms of Use, Privacy Policy, and Cookie Statement Through the contractual framework, we will identify the purposes according to which Qualtrics acts as a Controller and/or Processor.

A.2.1 General Terms and Conditions for Qualtrics Services ('GTC')

This section will describe the obligations and responsibilities of Qualtrics and education institutions mentioned in the General Terms and Conditions. The purpose of this documentation is to establish expectations for using the Qualtrics products and protecting the company from legal liabilities and government user interaction (in case of government requests). Qualtrics directly concludes the GTC with education institutions. SURF reviewed some of the GTC concluded directly with the members (education institutions).

The 'GTC' mentions the definition of the terms customer data and personal data:

- ***"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.

In addition to the GTC, Exhibit A provides a sample Data Processing Agreement for Qualtrics Services. The definition of personal data mentioned in the DPA is provided below:

- ***"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

²¹ Qualtrics answers shared with SURF on the 9th December 2025.

²² Qualtrics answers shared with SURF on the 9th December 2025.

*the Cloud Service; or (b) supplied to or accessed by Qualtrics or its Subprocessors to provide support.*²³

In the GTC, the roles and responsibilities regarding customer and personal data are defined:

- **Customer data:** as between the parties, Customer is responsible for the content and accuracy of the Customer Data.
- **Personal data:** Customer will collect and maintain all personal data contained in the customer data in compliance with applicable data protection and privacy laws.

The documentation makes it explicit that Qualtrics, as the data processor, acts only on the documented instructions of the Customer (the data controller) concerning the processing of Personal Data and does not determine the purpose or means of such processing.

Clause 3.4 in the GTC grants Qualtrics a right *‘to 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.’* Although this clause relates to the data processing activity, it is placed outside of the Data Processing Agreement.

Regarding the feedback feature, clause 12.12 states that Customer may, at its sole discretion, provide Qualtrics with Feedback, in which case Qualtrics and its Affiliates may retain and freely use such feedback without restriction. Customer is not responsible for Qualtrics’ use of any feedback. This means that the Customer bears no responsibility for how the recipient uses that feedback. This statement clarifies that any further use of the feedback (whether for product development, or other purposes) is solely under Qualtrics’ control. If the feedback includes personal data, the recipient is acting as a separate data controller for the feedback data. Because Qualtrics, according to the abovementioned clause, might use this data for their own purposes such as improving the feedback.

Qualtrics’ explains that the feedback does not include the ‘Customer Data’, and it is irrelevant for the DPIA.²⁴

In clause 12.10 of the GTC, the Governing Law for the disputes arising from the agreement is under the laws of the State of Delaware. *‘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.’*²⁵ No alternatives were observed for the jurisdiction; for example, to be placed in the EU.

²³ Qualtrics, ‘Qualtrics General Terms and Conditions & Data Processing Agreement Template’ (Qualtrics Success, 25 May 2023) <https://success.qualtrics.com/rs/542-FMF-412/images/Qualtrics%20GTC%20DPA%20%28for%20Online%29%20Template%20250523-MJR.pdf?version=0> accessed 10 October 2025.

²⁴ Qualtrics’ feedback from the 20th February 2026.

²⁵ <https://success.qualtrics.com/rs/542-FMF-412/images/Qualtrics%20GTC%20DPA%20%28for%20Online%29%20Template%20250523-MJR.pdf?version=0> Section 12.10 of the GTC.

Potentially, the mentioned jurisdiction choice misleads the customer to believe that only foreign law is applicable in case of disputes. Nevertheless, according to the case of the European Court of Justice ('CJEU'), *'the national court power to determine of its own motion whether a term is unfair must be regarded as constituting a proper means both of achieving the result ... preventing an individual consumer from being bound by an unfair term.'*²⁶

Even though the GTC are governed by the laws of the State of Delaware, the courts should be able to examine the clauses in consumer's home country. This will be applicable if the clause is misleading for the EU consumers.

A.2.2 Data Processing Agreement for Qualtrics Services

Exhibit A details the Data Processing Agreement ('DPA') for Qualtrics' customers. This example of the DPA together with the GTC is available publicly.²⁷

In the Schedule 1 of this agreement, SURF studied the subject matter and details of processing of Qualtrics services. It mentions the details for the processing of the customer, provider (Qualtrics), and details of the processing.

For the details of the processing and specification of the categories of data subjects, it is stated in the Schedule 1 that Customers determine the personal data for the specific data processing activities. No specific information was provided about the categories of data subjects and personal data to be processed by Qualtrics except for the personal data mentioned in the next paragraph. Qualtrics mentions its role as only a data processor, and mentions that the data processing scope is determined by Customers or Permitted Controllers²⁸:

*"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."*²⁹

This approach is determined by the fact that Qualtrics is a data agnostic platform, and Qualtrics communicated to SURF that *'the precise categories of Personal Data (which is a subset of*

²⁶ Joined Cases C-240/98 to C-244/98 *Océano Grupo Editorial SA v Roció Murciano Quintero* [2000] ECR I-4941' <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61998CJ0240>, para 28.

²⁷ Qualtrics, 'Qualtrics General Terms and Conditions & Data Processing Agreement Template' (Qualtrics Success, 25 May 2023) <https://success.qualtrics.com/rs/542-FMF-412/images/Qualtrics%20GTC%20DPA%20%28for%20Online%29%20Template%20250523-MJR.pdf?version=0> accessed 10 October 2025.

²⁸ 'Permitted Controller' means any other Controller authorized by Customer under the Agreement. See Exhibit A Data Processing Agreement in Section 1 Definitions.

²⁹ Schedule 1 DPA, Qualtrics, 'Qualtrics GTC DPA (for Online) Template' (no date) <https://success.qualtrics.com/rs/542-FMF-412/images/Qualtrics%20GTC%20DPA%20%28for%20Online%29%20Template%20250523-MJR.pdf> accessed 17 March 2026.

Customer Data) processed at any given moment depend solely on the Customer's use case and the configuration of the Cloud Service.³⁰

Regarding the purposes of the data processing, the Schedule 1 of the DPA outlines the following 'nature of the processing' when transferring personal data:

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.

The processing activities mentioned in the DPA involve core data handling actions of Qualtrics for the Customers. It outlines that Qualtrics acts solely as a data processor, operating under the instructions of the customer and within the scope defined by the service agreement, thereby aligning with data protection obligations governing processor responsibilities. Schedule 1 of the DPA states that the purpose of the transfer (the purpose of the processing) is to provide and support the Cloud Service and any associated services. Qualtrics and its Subprocessors may support the Cloud Service data centres remotely.

One of the purposes, where the line between the responsibilities of the vendor is blurred is purpose 5: 'Service development: release, development, and upload of any fixes or upgrades to the Cloud services'. Qualtrics informed to SURF that *'In summary, for the purpose of "Service Development," Qualtrics only uses a subset of Customer Data (Anonymized and Aggregated Analyses) that no longer constitutes Personal Data, effectively preventing any "intersection" with its controller purpose of "research and development" which uses its own collected data.'*³¹ Anonymising the customer data is a processing activity which Qualtrics seems to carry out for its own purposes outside the DPA.

In the DPA, the data processes are mentioned, and these purposes are mapped to the purposes which Qualtrics acts as an independent controller, as outlined section A.3.2 Qualtrics' Purposes as a Controller. This DPA outlines the roles of its customers (educational institutions) and Qualtrics, where customers are the sole data controllers.

³⁰ Qualtrics answers shared with SURF on the 9th December 2025.

³¹ Qualtrics answers shared with SURF on the 9th December 2025.

At this moment, it is challenging to determine the main purposes of the data processing based solely on the DPA. The agreement mentions general clauses instead of providing more specific information such as: *‘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.’*³² This statement provides some scope for the Customer to determine the extent of the processing; however, in practice, it offers no specific details about the processing due to the lack of specification of the parties’ roles, categories of personal data and the required level of accuracy. The broad applicability of the terms of the agreement should respect GDPR principles including purpose limitation, data minimisation, lawfulness according to Article 5 GDPR and ECJ (European Court of Justice) case-law.³³

For the special categories of personal data, the DPA mentions that: *“If Customer or a Permitted Controller intends to collect Special Categories of Personal Data, it will be specified in the applicable Order Form.”* SURF communicated to Qualtrics that this information should be governed by the DPA, however Qualtrics choice was that *‘Order form is subject to the DPA’*.³⁴ Additionally, Qualtrics mentioned:

*‘SCC Requirements (Template Consistency): Schedule 1 of the DPA follows the same framework as Annex I of the EU Standard Contractual Clauses (SCCs), which requires the parties to identify "special" categories of personal data transferred. Including a section for Special Categories of Personal Data in Schedule 1 is necessary to match the required structure of the EU SCC template. Since the SCC Annex requires this detail, Qualtrics uses the OF as the mechanism to capture that detail for the specific services being purchased.’*³⁵

The role of Qualtrics during the DPIAs is mentioned in Section 4.6 of the DPA: *“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.”*

Overall, the DPA stated that Qualtrics acts solely as a data processor, while education institutions are controllers and convey the use cases and the configuration of the Cloud Service.

A.2.3 Data Processing Agreement (DPA) with Educational Institutions (SURF agreement)

Educational institutions conclude a DPA with Qualtrics in two ways:

³² Qualtrics, ‘Qualtrics GTC DPA (for Online) Template’ (no date) <https://success.qualtrics.com/rs/542-FMF-412/images/Qualtrics%20GTC%20DPA%20%28for%20Online%29%20Template%20250523-MJR.pdf> accessed 17 March 2026.

³³ The ECJ reinforced that data minimisation and purpose limitation are not just guidelines, but enforceable obligations. Case C-446/21 Maximilian Schrems v Meta Platforms Ireland Limited [2024] EU:C:2024:834.

³⁴ Minutes of the Meeting with Qualtrics MOM from the 2nd of December 2025.

³⁵ Minutes of the Meeting with Qualtrics MOM from the 2nd of December 2025.

- 1) Have a direct DPA between educational institutions and Qualtrics. This DPA is accessible directly from the Qualtrics website. This is the DPA which was mentioned in A.2.2 Data Processing Agreement for Qualtrics Services.
- 2) A few educational institutions have a DPA through a third-party [REDACTED]. The DPA with educational institutions is not concluded between Educational institutions and Qualtrics directly, but between Qualtrics services reseller [REDACTED] and Educational institutions.

In article 2 of the DPA (via the reseller [REDACTED]), it is stated that the controller (educational institutions) assigns and instructs the processor to process the personal data on behalf of the controller.³⁶ According to the DPA, not only Qualtrics can be processor, but [REDACTED] as well. In the Qualtrics' GTC, it is stated that '(1) Partner will enter into a data processing agreement with Customer ("Customer DPA") that, in each case to the extent applicable: (A) allows Partner to use Qualtrics as a sub-processor of Personal Data;".³⁷ In this contractual relationship, Qualtrics is a subprocessor, and the Reseller is a Processor.

In the Annex to the DPA, there is the section where Customers (Controllers) give Qualtrics clear instructions from customers with a detailed description of the data processing including purposes, data subjects and categories, frequency of audits, retention periods of the personal data or the criteria for determining this. The scope of the agreement is determined per Customer's purposes and the corresponding Processor's services offered to the Customer.

The controller also gives the Processor specific permission for the transfer to third countries or international organisations. This information is mentioned on the separate Annex to the agreement. It is stated that '*Transfers to Subprocessors will be on the same basis as set out in the DPA*'.³⁸ Schedule 3 to the DPA mentions the EU transfers which are governed by the EU Standard Contractual Clauses, Swiss transfers and UK transfers (each party will be deemed to have signed the 'UK Addendum to the EU Standard Contractual Clauses'.³⁹

SURF analysed the DPAs available for the review (DPA publicly available and SURF model). Based on the information, it is difficult to map the categories of personal data to the matching specific purposes. The EDPB in their guidelines clearly states: '*It should also be noted that, "in accordance with Article 5 GDPR, the controller bears the burden of proving that data are collected, inter alia, for specified, explicit and legitimate purposes and that they are processed lawfully, fairly and in a transparent manner in relation to the data subject"*'.⁴⁰

³⁶ Data Processing Agreement 'Online Collaboration tools' based on SURF Model processing Agreement version 3.0 from January 2019 (date 24th October 2023), article 2.3.

³⁷ Qualtrics, 'Qualtrics GTC DPA (for Online) Template' (no date) <https://success.qualtrics.com/rs/542-FMF-412/images/Qualtrics%20GTC%20DPA%20%28for%20Online%29%20Template%20250523-MJR.pdf> accessed 17 March 2026.

³⁸ Schedule 1 to the Data Processing Agreement.

³⁹ Schedule 3 to the Data Processing Agreement.

⁴⁰ European Data Protection Board, *Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR* (European Data Protection Board, 8 October 2024) https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf accessed 30 July 2025, page 4.

The DPA concluded between Educational Institutions and [REDACTED], where Qualtrics is referenced, makes [REDACTED] and Qualtrics both processors. Therefore, it might be challenging to determine specific obligations of Qualtrics in the role of a data processor when another third-party reseller is included in the agreement.

A.2.4 Qualtrics Privacy policy

Qualtrics' privacy policy explains their data processing purposes. This documentation does not apply to personal information that Qualtrics processes on behalf of its customers, such as information using the Qualtrics XM Platform.⁴¹ The purposes that include the personal information that is processed on behalf of the Education institution is discussed in the section A.2.2.

The Privacy Policy identifies processing purposes that Qualtrics acknowledges in its role as a controller. These purposes are specified for the processing of personal data of the business customer representatives, website visitors and other users in connection with Qualtrics' website and services. Qualtrics states that the personal information that is processed on behalf of customers falls outside this Privacy Policy.⁴²

According to the Privacy policy, Qualtrics considers itself as the controller for processing activities in service of the following purposes:

- 1) To provide the services;
- 2) To communicate with the client about the services;
- 3) To improve, monitor, personalise, and protect the services;
- 4) For research and development;
- 5) For marketing and advertising;
- 6) For compliance and protection;
- 7) To train artificial intelligence tools.

The last purpose mentioned in Privacy Policy where Qualtrics might use personal information to train AI models is legally and ethically complex. It is essential to be transparent about the use of these AI tools, apply data minimisation and anonymisation techniques carefully, secure the data properly, and provide opt-out or consent options, where applicable. This will be further discussed in Part B.

Regarding marketing and advertising purposes, Qualtrics mentions in the Privacy Policy that:

*'Except where consent is required, we undertake such marketing and advertising on the basis of our legitimate business interests. Where we seek your consent, you may withdraw your consent at any time.'*⁴³

⁴¹ Qualtrics, *Privacy Statement* (Qualtrics, last updated 11 April 2025) <https://www.qualtrics.com/privacy-statement/> accessed 30 July 2025.

⁴² Qualtrics, 'Privacy Statement' (Qualtrics, 10 October 2025) <https://www.qualtrics.com/privacy-statement/> accessed 10 October 2025.

⁴³ Qualtrics, *Privacy Statement* (Qualtrics, last updated 11 April 2025) <https://www.qualtrics.com/privacy-statement/> accessed 30 July 2025.

This statement reflects that in case the legitimate interest arises, Qualtrics should justify and document when the specific data processing legal basis is permitted. Furthermore, this claim can be understood as Qualtrics carrying out certain marketing and advertising activities asking for user consent, or not asking for the consent when those actions might be deemed to be in its 'legitimate business interests'. This interpretation will be further discussed in the analysis of legal basis of the processing of personal data further in this DPIA and assessed if this commercial interest can fall within the legitimate interest.⁴⁴

A.2.5 Cookie Statement

Qualtrics' corporate website utilizes cookies and similar tracking technologies to support core site functionality, user experience, and analytics. The use of these cookies is governed by the **Qualtrics Cookie Statement**, which outlines the types of cookies used, their purposes, and the options available for user control.⁴⁵

Scope of cookie use

The statement applies specifically to Qualtrics' corporate websites, not to cookies used within the Qualtrics XM Platform by customers' users creating surveys or to survey respondents.

User control and consent

According to the statement, users can manage their cookie preferences through the site's cookie banner or browser settings. The lay out of the cookie statement describes the cookie use as compliant with applicable data protection regulations, including GDPR, by offering opt-out mechanisms and clear notice. Nevertheless, Qualtrics states that disabling cookies may impact the availability of certain features. SURF conducted an analysis of the cookies that Qualtrics uses in the Section A.7 Cookie Statement. SURF's technical research demonstrated that some of the cookies that were encountered were not mentioned in the Cookie Statement.

⁴⁴ Case C-621/22 Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens [2024] EU:C:2024:858.

⁴⁵ Qualtrics, *Cookie Statement* (Qualtrics, last updated 12 March 2024) <https://www.qualtrics.com/cookie-statement/> accessed 30 July 2025.

A.3 Data Processing Purposes

This chapter is about the purposes that Qualtrics processes users' personal data for. Listing these purposes will give a general idea of what the product is used for.

A.3.1 HORA Purposes as determined by Institutions

In addition to the purposes as described by Qualtrics, the purposes described below are based on descriptions of the different CoreXM/DesignXM modules and the research into the actual processing operations. They are divided into purposes based on the functions described in the 'Higher education reference architecture' model (HORA)⁴⁶. The HORA is a business function model for higher educational organisations. It describes the functions of an organisation, independently of how these functions are implemented in a specific organisation. Since the HORA describes the essential functions of educational organisations on a high level, it is a good model to derive from the main purposes for data processing in applications like Qualtrics. Using the HORA as a reference also ensures that it will be easy for institutions to find the right place in their organisational structure to implement any measures or changes from this DPIA. Note that the purposes and functions of the HORA model are exclusively available in Dutch.

Purpose	Function	Description
Applicatie-ontwikkeling	Informatie en Technologiemanagement	Developing application software and data collections.
Interne communicatie	Communicatiemanagement	Providing information to participants and employees.
Externe communicatie	Communicatiemanagement	Providing information to external parties.
Gegevensbeheer	Informatie en Technologiemanagement	Ensuring that high-quality data is available.
Gegevensverwerking en -analyse	Onderzoeksuitvoering	Processing (extracting, converting, cleaning, organising, etc.), analysing and interpreting the research data collected.
Identiteitenbeheer	Informatie en Technologiemanagement	Managing and making available data on users and their authorisations.
Informatiebeveiliging	Informatie en Technologiemanagement	Ensuring the continuity of information and the provision of information and limiting the possible consequences of

⁴⁶ Bedrijfsfunctiemodel (detail) (HORA2 wiki) [https://hora.surf.nl/index.php/Bedrijfsfunctiemodel_\(detail\)](https://hora.surf.nl/index.php/Bedrijfsfunctiemodel_(detail)) geraadpleegd op 30 juli 2025 (in Dutch only)

		security incidents to an acceptable, predefined level.
Informatiemanagement	Informatie en Technologiemanagement	Shaping, directing, adjusting, monitoring and maintaining the information provision at strategic and tactical levels.
Kwaliteitszorg Onderzoek	Verantwoording	Evaluating whether research meets the quality criteria set for it, and reporting and accounting for this (externally). This includes evaluations in accordance with the Standard Evaluation Protocol as established by VSNU, KNAW and NWO, but also other evaluation frameworks such as the Shanghai index and citation indices.
Marktbewerking	Deelnemerwerving	Carrying out specific actions and campaigns to reach target groups such as organising information days and events for participants.
Onderzoeksplanning	Onderzoeksontwikkeling	Preparing a proposal for a research study and submitting it for approval.
Onderzoeksuitvoering	Onderzoeksontwikkeling	Conducting a careful, verifiable and systematic study of a particular issue to answer research questions.
Performancemanagement	Verbetermanagement	Ensuring that the functioning of the organisation is in line with previously set objectives.

Table 1 HORA business processes fulfilled with Qualtrics

A.3.2 Qualtrics' Purposes as a Controller

It was discussed in section A.2 Contractual that Qualtrics acts as a processor for the personal data and purposes assigned to it by education institutions according to the DPAs.

In this section, SURF will elaborate on purposes according to which Qualtrics acts as a Controller. These purposes are described in the Privacy Policy,⁴⁷ where Qualtrics collects data for its own purposes, such as information from website visitors, or any other processed determined by Qualtrics.

Purpose
1) To provide the services; 2) To communicate with the client about the services; 3) To improve, monitor, personalise, and protect the services; 4) For research and development; 5) For marketing and advertising; 6) For compliance and protection; 7) To train artificial intelligence tools.

Table 2 Qualtrics' data processing purposes

⁴⁷ Qualtrics, 'Privacy Statement' (11 April 2025) <https://www.qualtrics.com/privacy-statement/> accessed on the 30th of January.

A.4 Processed Personal Data

A.4.1 Personal Data Definition

According to article 4(1)(a) of the GDPR,

“‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

To explain privacy risks of data processing operation, it is important to consider what types of data of which groups of data subjects are being processed.

This section will describe all personal data being processed from different categories of data subjects in Qualtrics’ documentation. In the Section Personal Data in Privacy policy, we will classify these personal data by categories mentioned by Qualtrics. For each category of personal data, we indicate which personal data are collected and processed. This section concludes with a subsection on the DSARs.

A.4.2 Personal Data in Privacy policy

The Privacy Policy mentions the type of personal data processed by Qualtrics for customer representatives, website visitors, and other users interacting with Qualtrics’ websites and services.⁴⁸ The types of personal data categories are within the scope of the this privacy policy. The Privacy Policy does not cover data processed on behalf of customers via the XM Platform and it is outside of the scope of this DPIA. However, it was necessary to examine the personal data covered under the Privacy policy to start categorising the known personal data, since Qualtrics refused to provide SURF with this information.

1. Personal Information Provided by a Customer:

- Contact and account details such as name, email, phone number.
- Financial/payment info: bank details, transaction history.
- Communication records: feedback or support inquiries.
- Marketing preferences and engagement data.

2. Automatic Data Collection:

- Device details such as IP address, OS, browser type, location.
- Online activity such as pages viewed, time spent, navigation paths.
- IP addresses from survey respondents to prevent fraud and ensure security.
- Session replays on Qualtrics’ website (excluding IP addresses and masked text input) to improve user experience.

3. Third-Party and Social Media Sources:

- Data from social platforms and other sources like marketing partners or public databases.

⁴⁸ Qualtrics, *Privacy Statement* (Qualtrics, last updated 11 April 2025) <https://www.qualtrics.com/privacy-statement/> accessed 30 July 2025.

4. Call Recordings:

- Certain calls may be recorded to enhance service quality, resolve disputes, train staff, and maintain accurate records.

A.4.3 Data Processing Agreement personal data list

A DPA applies to all Qualtrics services such as Cloud services, professional services, and research services.⁴⁹

The details of the processing and categories of data subjects, personal data, and special categories of personal data are mentioned briefly in the DPA, but in a quite general overview of the possible categories of data processed.

Mainly, in the Schedule 1 'Subject Matter and Details of Processing', it is mentioned that Customers determine the nature and scope of personal data transferred or processed in the cloud service. This includes what data is stored, transmitted, or otherwise processed. Additionally, it is stated that it must be explicitly stated in the applicable Order Form if any special categories of personal data are to be processed. Qualtrics further describes that additional measures are implemented by Qualtrics when special categories of data are transferred such as training of personnel, encryption of data in transit and at rest, and system access logging and general data access logging.

Below in Table 3 Qualtrics' DPA details of processing, SURF shows the details of processing for the Qualtrics services.

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.
-----------------------------	---

⁴⁹ Qualtrics, 'General Terms and Conditions and Data Processing Agreement' (25 May 2023) <https://success.qualtrics.com/rs/542-FMF-412/images/Qualtrics%20GTC%20DPA%20%28for%20Online%29%20Template%20250523-MJR.pdf> accessed 30th January 2026.

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 / authorisation 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 Order 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.

Table 3 Qualtrics' DPA details of processing

A.4.4 Categorised personal data by SURF from Privacy Policy

It is important to understand the full picture of the type of personal data that is processed by Qualtrics in the role as the controller according to the Privacy Policy.⁵⁰

Category	Description	Data Subject Category	Sensitivity Classification (GDPR)
Personal Information Provided	Name, email, phone number; Bank details, transaction history; Feedback or support inquiries; Marketing preferences and engagement	Customer / Consumer	Personal Data (Standard)
Automatic Data Collection	IP address, OS, browser type, location; Page views, time spent, navigation paths; IP addresses in surveys; Session	Website Visitor / Survey Respondent	Personal Data (Standard; some pseudonymized)

⁵⁰ <https://www.qualtrics.com/privacy-statement/>

	replays (excl. IP & masked inputs)		
Third-Party & Social Media Data	Social platform data; Data from marketing partners or public databases	Social Media User / Public Data Subject	Personal Data (Varies based on source and content)
Call Recordings	Recorded conversations for quality, dispute resolution, training, and record-keeping	Caller / Customer	Personal Data (May contain special categories depending on context)

Table 4 Privacy Statement categories of personal data (Qualtrics as a controller).

A.4.5 Combined personal data from the DPA and Privacy Policy

The information from the Privacy Statement and Qualtrics' DPA lacked the concrete information about the exact list of personal data processed on behalf of Qualtrics in the roles either as a controller or processor. During the communication between Qualtrics and SURF, Qualtrics specified that they are a data agnostic platform. This means that *'all Customer Data is treated as confidential and is protected equally regardless of its content, and Qualtrics does not classify the data. This standardized protection ensures that even if sensitive data is involved, it receives the same industry-best security measures. By committing to processing only at the Customer's instruction and by ensuring that the only data derived from Customer Data used for development is de-identified and aggregated, Qualtrics maintains a clear separation between its roles as processor and controller.'*⁵¹

Given the nature of the services that Qualtrics provides to the education institutions and lack of the overview information that is publicly available, SURF mapped the list of categories of personal data based on the types of personal data that Qualtrics processes on behalf of the controller (education institution) as a processor.

Below, SURF mapped the data subject categories with the purposes of processing according to the data processing agreement between education institutions and Qualtrics. This is the list processing other than the processing which was mentioned in the abovementioned Table 4 .

Category	Description	Data Subject Category	Sensitivity Classification (GDPR)	Purpose
Identification data	Name, system access/usage/authentication data.	Customer / Consumer	Personal Data (Standard)	Processed according to the instructions of the Controller (education institutions);

⁵¹ Qualtrics response to SURF questions from the 9th of December 2025.

				Data storage & Backup
Contact data	Phone numbers, email address, address data.	Customer/Consumer	Personal Data (Standard; some pseudonymized)	User Communication – Communication to Authorised users.
Technical data/Usage data/Diagnostic data	System access/usage/authorization data.	Consumer	May contain personal data, if some of this information may relate to an identified or identifiable person.	Service provisioning, Service development; Technical processing;
Usage Data	Application-specific data that Authorized Users enter into the Cloud Service.	Customer data/User data	May contain personal data	Service provisioning; Professional services.
Content data	Contract data, invoice data, and any application-specific data that Authorized Users transfer or enter into the Cloud Service.	Customer	May contain personal data	Service provisioning; Professional services.
Special categories of personal data	The processing of Special Categories of Personal Data is Determined by Customer or Permitted Controllers. Specifically: includes data concerning health, genetic data, biometric data, data revealing racial or ethnic origin, political opinions, religious	Customer	Personal data	Process in accordance with the Order Form signed between Qualtrics and customer.

	or philosophical beliefs, trade union membership, or data concerning a natural person's sex life or sexual orientation.			
--	---	--	--	--

Table 5 Personal data mapping for Qualtrics as a processor

For the personal data processed on behalf of the Customer, Qualtrics clarifies that the Customer is the Data Controller. Education institutions determine what data to collect and for what purposes. Qualtrics could not provide SURF with the list of personal data because of the confidentiality of other customers. Therefore, SURF could not access a more detailed documentation of specific categories of data subjects and personal data to be processed by Qualtrics.

All Data are controlled by Customers, who are designated as data controllers. Qualtrics is the data processor. Customers determine the following about the data stored in the Qualtrics platform:

- Which type of data to collect
- Who to collect data from
- Where to collect data
- What purpose
- When to delete the data

SURF requested documentation from Qualtrics to determine what type of data to collect and for what purposes. Qualtrics responded that they do not share a list of personal data that the vendor received from other customer due to confidentiality reasons.⁵² This was the response despite SURF mentioning that as an organisation, SURF represents the members in the educational sector.

⁵² Qualtrics response from the 11th of August 2025.

A.4.6 Question Types

Qualtrics supports several types of questions to enable researchers to gather the information in various formats that suits their research. Listed below is a summary of some of the question types.

Question Type	Description
Multiple Choice	Standard closed question type, presented as a list, dropdown, or select box.
Text Entry	Captures open-ended responses; can be short or long form.
Text / Graphic	Used to display static text, instructions, or images within a survey.
Matrix Table	Collects multiple data points in a tabular format; ideal for grouping similar questions.
Form Field	Captures standard form inputs such as name and email.
Calendar	Allows respondents to input dates and times using a calendar interface.
Slider	Uses a draggable bar to indicate preference or opinion.
Rank Order	Enables respondents to rank a list of items based on preference or priority.
Side by Side	Lets users answer multiple related questions in a condensed table layout.
Net Promoter Score® (NPS)	Standardised question measuring likelihood to recommend on a scale from 0 to 10.
Timing	Hidden question that records or limits the time a respondent spends on a survey page.
Graphic Slider	Similar to sliders, but uses visual elements (e.g. smiley faces or letter grades).
Constant Sum	Collects numeric input where the total must sum to a specified value; often used for time or budget allocation.
File Upload	Allows respondents to upload files, such as documents or images.
Pick, Group, and Rank	Allows items to be sorted into categories and ranked within those categories.
Drill Down	Multi-level dropdown menu that narrows choices from broad to specific.

Signature	Respondents draw their signature using a mouse or touch screen.
Heat Map	Respondents click parts of an image; heat maps show popular areas.
Hot Spot	Respondents select predefined regions within an image.
Meta Info	Hidden question that captures browser and operating system information.
Captcha Verification	Prevents bot submissions by verifying the respondent is human.
Highlight	Allows respondents to highlight and evaluate words in a block of text.
Screen Capture	Lets respondents upload screenshots of their current screen; available in Website/App Feedback projects.
Video Response	Respondents can record and submit video or audio responses. Also logs the user's location information.
Unmoderated User Testing	Collects respondent-recorded feedback through video or audio while interacting with a product or site.
Location Selector	Enables respondents to select a geographic location from a predefined list.
ArcGIS Map	Allows geographic selection from an ArcGIS-integrated map; can pass the data to ArcGIS directly.
Solicit Reviews	Enables respondents to submit reviews to external platforms (e.g. Google, Facebook) directly from within the survey.
Tree Testing	Asks respondents to locate a specific web page using a simulated navigation menu; used for evaluating information architecture.

Table 6 Question Types available within Qualtrics

A.4.6.1 Meta Info

SURF analysed the question types. The Meta Info type was noteworthy, so this paragraph will give a bit more context about this question type. This feature is designed as a hidden question type that allows researchers to collect technical details about a respondent's environment without the survey recipient providing this information directly.

According to Qualtrics' technical specifications, the feature captures the following data points:

- Browser type and version;
- Operating system;
- Screen resolution;
- User agent strings;

In addition, SURF's technical testing observed that in addition to the above data points, location data is collected and displayed to researchers as well, derived via GeoIP estimation See Figure 1.

However, Qualtrics clarified that this data is not captured by the Meta Info question type, but is controlled by a survey-wide setting. Institutions can opt to disable collecting this data by enabling the 'Anonymise responses' option. See Figure 2.

Julian Rill

View Response

Q1. do you want to share all your data with us please?
here are the terms:

☐ No
☒ Yes

Browser: Firefox
Version: 146.0
Operating System: Mac OS
Screen Resolution: 1512x982
Flash Version:
Java Support:
User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:146.0) Gecko/20100101 Firefox/146.0

Q4. Click to write the question text

[1768468937.webm](#)
428.5KB
video/webm

Location Data

Location: [\(52.2975, 5.1587\)](#)

Source: GeoIP Estimation

Figure 1 Collected data from Meta Info Question Type

Anonymise responses

Don't record respondents' IP address, location data and contact info.

☐ Off

Figure 2 Anonymise responses option within survey settings

A critical aspect is the allocation of responsibility for transparency. Qualtrics adopts a firm stance that, as a data processor, they do not interact directly with data subjects regarding these technical collections. Consequently, the legal obligation to provide notice and obtain valid consent rests entirely with the institution (the controller).

Because the Meta Info question is hidden by default, respondents are typically unaware that their machine's metadata and estimated location are being collected unless the survey creator explicitly mentions it in a privacy statement or a consent form. During SURF's technical inquiries, Qualtrics confirmed that they do not provide an automatically generated consent form that details these specific machine-level processes. Institutions or researchers of institutions using Qualtrics must manually configure and write their own notices if they wish. Qualtrics instructs institutions to build a consent form manually using built in logic.⁵³

⁵³ Qualtrics – Building a Consent Form, URL: <https://www.qualtrics.com/support/survey-platform/common-use-cases-rc/building-a-consent-form/>

A.5 Data Processing Activities

This chapter outlines the types of processing activities that may occur within the Qualtrics platform. In accordance with Article 4, Paragraph 2 of the GDPR, “processing” is defined as follows:

“‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;”

It is important to bear in mind that the controllers determine the purposes and means. Therefore, the scope of the processing may vary based on the specific requirements of the institutions. The descriptions below go into more detail and are based on the actual processing operations as found in the research for this DPIA.

A.5.1 Identity and Access Management

Qualtrics' Identity and Access Management (IAM) framework is designed to provide security and offers various configuration possibilities for education organisations. Qualtrics operates on a principle of least privilege and need-to-know when assigning access rights to both its internal personnel and customer users.

A.5.1.1 Authentication Methods and Access Control

Qualtrics offers various authentication methods to provide the flexibility in managing user access.

Native Login: Users can log in with a username and password. Brand Administrators (BAs; as explained in A.5.1.1.1) can customize password requirements, including minimum length (e.g., 12 characters), complexity (at least three of uppercase, lowercase, number, or special characters), maximum age (e.g., 60 days), and password history (e.g., 12 previous passwords). Account lockout settings can also be configured, such as the number of failed attempts (e.g., 4 attempts) and the lockout period (e.g., at least 30 minutes). This method is not preferred as more secure alternatives exist.

Single Sign-On (SSO): Most education organisations utilise SSO, which allows users to log in using their own organisation's credentials. This can be implemented via a self-service portal or with Qualtrics' assistance. SSO is key to validating user affiliation with the university. SURFconext is one of the supported SSO providers.⁵⁴ When SSO is enabled, BAs can choose whether to allow or disable the Qualtrics Login as a fallback, thereby closing a back door for alternative login methods.

Multi-Factor Authentication (MFA): MFA is supported and can be enabled or disabled by the BA for the entire brand to provide an additional layer of security for logins.

⁵⁴ “SURFconext Key Rollover 2023: Procedure for Qualtrics - SURF IAM - SURF User Knowledge Base,” n.d.

<https://servicedesk.surf.nl/wiki/spaces/IAM/pages/128910221/SURFconext+key+rollover+2023+Procedure+for+Qualtrics>.

- Invitation-Only Access and Password Protection: Surveys can be configured to be available only by invitation or be password-protected to limit access to a known group of individuals.
- Referral Website Restrictions: BAs can configure surveys to only be accessible if the user comes from a specified referral website (like surf.nl) to prevent unauthorised access from other domains.
- IP Allowlisting: Customers can limit access to their Qualtrics instance to specific IP addresses.
- Session Management: BAs can set automatic logout based on inactivity (like 60 minutes) and define the maximum concurrent sessions per user (default 500). They can also view and end active sessions for users.

A.5.1.1.1 User Management and Permissions

The Qualtrics platform provides a hierarchical structure for user management, segregating administrator and user roles.

Administrator roles:

- Brand Administrator (BA): This is the highest level of permission within a Qualtrics license. BAs are responsible for moderating user activity, managing account access, setting up teams and divisions, and maintaining organisational and security settings. They have visibility across the entire brand and its divisions. BAs also have the ability to proxy login into user accounts, a feature which can be disabled by the BA but is enabled by default. More on proxy login in A.5.2.
- Division Administrator (DA): DAs have full administrative access but are restricted to their specific division only. They can see user activity and reports within their division but not across others. This allows for decentralised management while maintaining overall control by the main BA.

User roles:

- User Types: BAs can define custom "User Types", which are predefined sets of permissions outlining what a user can and cannot do. This automates the process of assigning permissions. For example, distinct user types can be created for students, faculty, or administrative staff, each with tailored access rights. Qualtrics also offers default user types that cannot be customised. Education organisations must create new user types to modify permissions. The default list of user types can be seen in Appendix 2.
- Groups: User groups are distinct from user types. A group is a collection of two or more users that can share projects, graphics, files, and messages in libraries. They are typically used for cross-collaboration between different divisions. Access to groups is defined by group assignments, not user types.

A.5.1.2 Provisioning and Deprovisioning Access

When it comes to provisioning users in Qualtrics, several options are available. BAs can manually create accounts by specifying usernames, passwords, divisions, and permissions. This process offers granular control but can be time-consuming at scale and increase the risk of user error. To streamline onboarding, there's a bulk upload feature that accepts CSV files which allows administrators to import multiple users simultaneously. More efficiently, Qualtrics supports automated, just-in-time provisioning when SSO is enabled. In such cases, user accounts are

created dynamically upon first login, with role and division assignments determined by attributes passed from the SSO provider. This setup reduces the need for ongoing manual input during provisioning.

However, deprovisioning and managing role changes present significant gaps. There is no automatic process to adjust or revoke user access when their role changes or they leave the organisation. If SSO access is lost (say, because someone exits the institution) their Qualtrics account remains active unless manually handled. BAs can either disable the account, which retains all associated data but still counts against license limits, or delete the account entirely after optionally transferring data. While brand settings can be configured to disable inactive accounts after a set period, this is a workaround rather than a robust deprovisioning mechanism.

Role changes are also not dynamically reflected. For institutions relying on SSO for user mapping at login, initial provisioning may align with current attributes, but subsequent updates to roles or permissions aren't automatically synchronised if the user did not need to re-login. Maintaining accurate role-based access requires ongoing manual oversight or the development of custom integrations using Qualtrics' API.

The API does support full user lifecycle operations (creating, updating, disabling, and deleting users) and enables automation via external systems. Education organisations can use this API to build integrations with identity platforms such as SailPoint or Okta for more centralised identity governance. While there is no out-of-the-box connector, the API provides a foundation to build such workflows.

A.5.2 Proxy Login

Qualtrics incorporates a proxy login functionality, which enables Brand Administrators to access and operate within other user accounts as if they were that user. This capability is enabled by default in the system, though Brand Administrators retain the option to disable it.⁵⁵ All actions performed through a proxy login are logged within the platform's activity logs.⁵⁶ These logs record details such as the date and time of the event, the user ID of the account into which access was gained and specifically identify the Brand Administrator who initiated the proxy session.⁵⁵ The end user whose account is accessed does not receive any notification that a proxy login has occurred.

A.5.3 Incomplete Survey Responses

Qualtrics provides functionality to manage incomplete survey responses to allow participants to finish their surveys later. For respondents accessing the survey via a personalised traceable link, if the customer chooses to set it up in this manner, progress is saved on Qualtrics' servers and remains accessible across different devices. This is the default behaviour, but institutions may divert from this behaviour, see Figure 3. However, for anonymous responses, progress is stored locally in browser cookies and is therefore tied to the specific device and browser used. SURF's technical testing confirmed this behaviour.

⁵⁵ Qualtrics. "Security Tab." Accessed June 27, 2025. <https://www.qualtrics.com/support/survey-platform/sp-administration/security-tab/>.

⁵⁶ Qualtrics, "Qualtrics' Cloud Security & Privacy Framework," April 2025.

Allow respondents to finish later

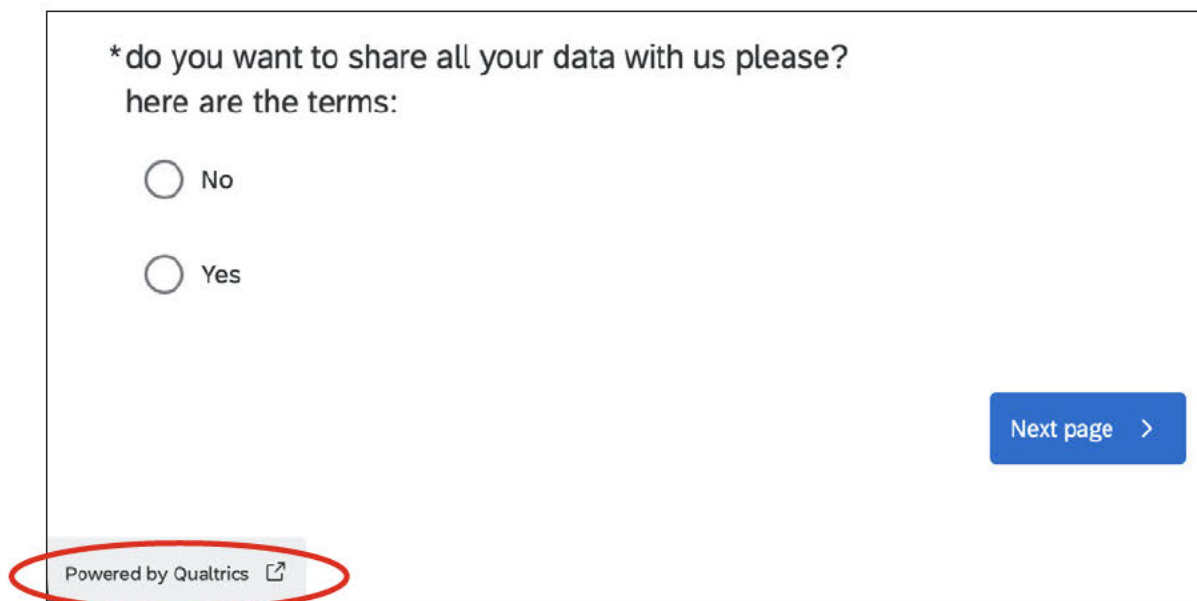
Let respondents using an anonymous link leave your survey and re-enter to finish it later. Respondents with a personalised link will still be able to stop and continue at a later time, even when this option is off.

☒ On

Figure 3 Survey setting saving respondent's survey data, enabled by default

Brand Administrators possess the capability to configure the handling of these incomplete responses, including setting a duration after which they are automatically recorded as submitted. By default, Qualtrics' system is configured to record incomplete responses after one week, meaning that even partially completed surveys will be captured and saved at that point. However, users are not automatically informed this setting has been configured. Survey creators need to explicitly denote this fact as part of the survey itself.

Qualtrics positions itself as a data processor, and the responsibility for informing participants about the handling, storage, and retention of incomplete responses lies squarely on the educational organisations acting as data controllers. Although Qualtrics offers a so-called "standard disclaimer" within surveys⁵⁷ (see Figure 4), it is limited to a generic link to the Qualtrics.com website, which simply describes what Qualtrics is and outlines general survey-related services. It does not explain how data from incomplete surveys is handled or retained.



* do you want to share all your data with us please?
here are the terms:

☐ No

☐ Yes

Next page >

Powered by Qualtrics [↗](#)

Figure 4 Standard disclaimer on survey provided by Qualtrics (circled in red)

This minimal default disclaimer places a significant burden on institutions to design their own meaningful and transparent notices. Qualtrics does not provide templates, guidance, or embedded warnings by default to assist educational organisations in meeting their legal obligations regarding informed consent or data retention disclosures.

⁵⁷ Meeting between Qualtrics and SURF on March 23rd, 2025

A.5.3.1 Technical Investigation of Data Flows and Endpoints

We conducted a network-level technical investigation based on scripted scenarios in our own testing environment provided by Qualtrics, which in turn are based on real-world usage of educational organisations (see Appendix 1). This means that all data flows which were detected between the testing device and Qualtrics' servers were logged and analysed. All mapped endpoints (servers and devices which any data using Qualtrics' services flows to and from) can be consulted in Appendix 3.

Our technical investigation identified multiple endpoints and their associated registrars, which we then matched against Qualtrics' disclosed subprocessor list (as described in A.8.3). Qualtrics categorises its subprocessors into four groups: mandatory, optional for technical functionality, optional for professional services, and affiliated entities. Our investigation revealed several important observations that diverge from the documented data processing arrangements, particularly concerning data residency and third-party services.

A.5.3.2 Google Analytics and Google Tag Manager

While Google, LLC is listed as an optional subprocessor for "AI capabilities, including translation services", and SURF didn't opt for these AI capabilities during testing, the mapped endpoints frequently include domains related to Google Analytics (region1.google-analytics.com, www.google-analytics.com) and Google Tag Manager (www.googletagmanager.com). The specific purpose of web analytics or tag management is not mentioned in Google's listed services, which primarily focus on AI and translation. This suggests an unlisted function for a recognised subprocessor.

A.5.3.3 Pendo

Qualtrics states that "Pendo is not a subprocessor. It does not process customer data."⁵⁸ However, SURF observed several POST request to data.pendo.io, which represent the transmission of compressed behavioral telemetry and session metadata from the Qualtrics environment to the Pendo analytics platform. Based on the request headers and the structure of the Gzipped JSON payload, SURF observed that the data processed includes technical identifiers such as the user's operating system (macOS 10.15.7), browser version (Chrome 138), and unique session tokens. Furthermore, the presence of an encoded "events" string indicates the collection of granular clickstream data, such as specific UI interactions, page navigation paths, or time-on-page metrics. SURF assumes that while the payload identifies the specific application via the API key 1a296aed..., it likely associates these actions with a pseudonymized user ID to track the end-to-end journey within the survey interface.

A.5.3.4 Amplitude

Qualtrics states that "Amplitude is not a subprocessor. It does not process customer data."⁵⁹ However, SURF observed many POST requests to Amplitude, which function as high-fidelity event tracking for the Qualtrics TextIQ analytics suite. The data processed through these endpoints is significantly more granular than standard web logs, containing explicit internal identifiers including a persistent User ID (UR_br8tOP1eA4UWi8u) and a unique Device ID.

⁵⁸ Qualtrics' review on SURF's DPIA, 20 February 2026

⁵⁹ Qualtrics' review on SURF's DPIA, 20 February 2026

The JSON payloads reveal the systematic collection of functional interaction data, specifically documenting user engagement with the TextIQ interface, such as “PageLand” events and “Response.View” actions. Of particular note for this assessment is the processing of operational metadata linked to specific survey responses (responselds like R_25tDs3LI3TxoJct), sentiment analysis configurations (is5LevelSentiment), and linguistic settings.

While the IP address is masked in the payload as \$remote (indicating it is captured at the server level rather than the client level), the combination of precise timestamps, session IDs, and the specific survey IDs (e.g., SV_3yljFElimPrABSK) enables the reconstruction of a highly detailed user behavioural profile. These logs confirm that third-party analytics are being used to monitor not just that a user is present, but the specific data subsets and analytical tools they are interacting with within the Qualtrics platform.

A.5.4 Data Subject Access Requests

As part of the technical investigation, we conducted a targeted evaluation of Qualtrics’ capacity to support and comply with data subject rights, specifically the right of access under Article 15 of the GDPR. The approach involved the submission of formal DSARs from multiple actors who had interacted with the Qualtrics platform in a variety of scripted testing scenarios, as described in Appendix 1.

These actors included test profiles simulating researchers with user accounts, administrative users, and survey participants. Each actor engaged with the platform in ways representative of real-world use cases, such as designing and deploying surveys, responding to survey instruments, managing survey projects, and reviewing analytics. The objective was to establish whether Qualtrics offers adequate mechanisms for facilitating access to personal data held about users and respondents, and to determine the scope of data retrievable under a standard DSAR procedure.

A.5.4.1 Submission of DSARs

Each DSAR was set up to seek a full disclosure of personal data processed by Qualtrics in connection with the specific identity of each test actor. The requests included standard elements typically associated with such submissions, such as the requestor’s name, email address, and IP address. The content of the requests followed GDPR Article 15 requirements and specifically sought:

- A copy of all personal data traceable to the data subject, including data stored in Qualtrics systems, logs, and other records
- The purposes for which the data is being processed
- The categories of personal data concerned
- The recipients or categories of recipients to whom the data have been or will be disclosed, particularly in third countries or international organisations
- The envisaged retention period or the criteria used to determine such a period
- The source of the data if it was not collected directly from the data subject
- The available options for rectification, erasure, or objection, and the procedures involved
- The existence of any automated decision-making or profiling activities and the logic involved in such processes, along with their consequences for the data subject

A.5.4.2 Qualtrics' Response to DSARs

In response to each DSAR submitted, Qualtrics declined to provide a direct reply to the information requested. Their reasoning is that they only provide data subject access support for personal data which they state they are the controller for, even though the DPA does require them to assist the controller (SURF in this scenario) with DSARs.⁶⁰ Qualtrics referred the data subject to a publicly available self-service support page hosted on its website.⁶¹ This page provides guidance for users of the Qualtrics platform (typically researchers or administrators) on how to manually export survey response data.

The content of the support page pertains exclusively to the export of data collected from survey respondents. The export functionality described permits downloading of structured response data from surveys, including:

- Responses to survey questions
- Survey metadata (like start and end times, recorded date, IP address)
- Contact fields and embedded data submitted by respondents

Export options are limited to formats such as CSV, TSV, Excel, XML, SPSS, or Google Sheets. While this export mechanism allows for the retrieval of basic participant response data, it does not support access to:

- Personal data relating to Qualtrics user accounts (like researchers, administrators)
- Technical error reports or diagnostic data
- Administrative role-based access records
- Platform configuration or permission management data
- Internal system metadata associated with project use
- The retention period of the data types

In some cases, certain data are available to Brand Administrators for manual extraction. For example, they may be able to manually search authentication logs for a user's email address to determine if and when a login occurred.

A.5.5 Personal Data Request tool

SURF obtained a new Qualtrics testing environment after the previous testing environment expired after multiple discussions between both parties. The new environment has access to the Personal Data tool, which is designed to assist with compliance regarding data subject access and deletion requests.⁶² The tool serves as a centralised search engine to locate personal information associated with specific email addresses across the institution's Qualtrics platform.

Records that can be located and/or deleted by email address include:

- Survey responses (all [recorded responses](#), including any incomplete survey responses that were closed)
- Distributions (excluding [personal/unique links](#))
- Partial survey responses ([responses in progress](#))

⁶⁰ Qualtrics Data Processing Agreement, Article 4.6.

⁶¹ Exporting Response Data, URL: <https://www.qualtrics.com/support/survey-platform/data-and-analysis-module/data/download-data/export-data-overview/>

⁶² Personal Data Tool, URL: <https://www.qualtrics.com/support/survey-platform/sp-administration/data-privacy-tab/right-to-erasure/>

- Contacts ([original](#) and [XM Directory](#))
- [Tickets](#)
- [Participants](#)
- [Users](#)

SURF's technical testing of the tool revealed a lack of any form of logging. Personal data often resides in logs through technical identifiers like IP addresses, usernames, and email addresses captured during routine server requests or authentication events. Application and error logs can be particularly risky, as they may accidentally record sensitive input data like full names, phone numbers, or even session tokens and passwords if a system crashes while processing a form. security audit logs link specific actions (such as survey access or account changes) directly to a user's identity.

While the Personal Data tool is used to manage and export specific records, the broader platform infrastructure lacks any form of logging for routine researcher, administrator, or other platform user activity. Specifically, the following findings were noted:

- **Read Access and Modification Logs:** The tool does not export detailed logs showing when researchers or users access, view, or modify survey response data. There is no transparent record of which individuals have interacted with specific data points within a project.
- **Authentication and Session Logs:** Testing indicated that logs for user authentication and active sessions, tracking when and how researchers log in to the Qualtrics platform, are not accessible or provided within the tool.

Example response data of [Julian.rill@surf.nl](#) (Brand Administrator) new testing environment (note: does not contain full scenarios as they were not retested):

```
{
  "julian.rill@surf.nl": {
    "responses": [
      {
        "StartDate": {
          "Label": "Start Date",
          "Value": "2026-01-15 09:21:48"
        },
        "EndDate": {
          "Label": "End Date",
          "Value": "2026-01-15 09:22:21"
        },
        "Status": {
          "Label": "Response Type",
          "Value": "IP Address",
          "IPAddress": {
            "Label": "IP Address",
            "Value": "178.229.191.249"
          },
          "Progress": {
            "Label": "Progress",
            "Value": 100
          },
          "Duration (in seconds)": {
            "Label": "Duration (in seconds)",
            "Value": 32
          },
          "Finished": {
            "Label": "Finished",
            "Value": "True"
          },
          "RecordedDate": {
            "Label": "Recorded Date",
            "Value": "2026-01-15 09:22:23"
          },
          "ResponseId": {
            "Label": "Response ID",
            "Value": "R_2DnLj2WEHgY0xop"
          },
          "RecipientLastName": {
            "Label": "Recipient Last Name",
            "Value": "Rill"
          },
          "RecipientFirstName": {
            "Label": "Recipient First Name",
            "Value": "Julian"
          },
          "RecipientEmail": {
            "Label": "Recipient Email",
            "Value": "julian.rill@surf.nl"
          },
          "ExternalReference": {
            "Label": "External Data Reference",
            "Value": ""
          },
          "LocationLatitude": {
            "Label": "Location Latitude",
            "Value": 52.2975
          },
          "LocationLongitude": {
            "Label": "Location Longitude",
            "Value": 5.1587
          },
          "DistributionChannel": {
            "Label": "Distribution Channel",
            "Value": "gl"
          },
          "UserLanguage": {
            "Label": "User Language",
            "Value": "EN-GB"
          },
          "Q1": {
            "Label": "do you want to share all your data with us please?\nhere are the terms:",
            "Value": "Yes"
          },
          "Q1_DO_1": {
            "Label": "do you want to share all your data with us please?\nhere are the terms: - Display Order - No",
            "Value": 1
          },
          "Q1_DO_2": {
            "Label": "do you want to share all your data with us please?\nhere are the terms: - Display Order - Yes",
            "Value": 2
          },
          "Q2_Browser": {
            "Label": "Click to write the question text - Browser",
            "Value": "Firefox"
          },
          "Q2_Version": {
            "Label": "Click to write the question text - Version",
            "Value": 146
          },
          "Q2_Operating System": {
            "Label": "Click to write the question text - "
          }
        ]
      }
    ]
  }
}
```

```
Operating System","Value":"Mac OS"},"Q2_Resolution":{"Label":"Click to write the question text
- Resolution","Value":"1512x982"},"Q2_DO_1":{"Label":"Click to write the question text - Display
Order - Browser","Value":""},"Q2_DO_2":{"Label":"Click to write the question text - Display
Order - Version","Value":""},"Q2_DO_3":{"Label":"Click to write the question text - Display Order
- Operating System","Value":""},"Q2_DO_4":{"Label":"Click to write the question text - Display
Order - Screen Resolution","Value":""},"Q2_DO_5":{"Label":"Click to write the question text -
Display Order - Flash Version","Value":""},"Q2_DO_6":{"Label":"Click to write the question text -
Display Order - Java Support","Value":""},"Q2_DO_7":{"Label":"Click to write the question text -
Display Order - User Agent","Value":""},"Q6_Id":{"Label":"sign here, or else... -
ID","Value":""},"Q6_Name":{"Label":"sign here, or else... -
Name","Value":""},"Q6_Size":{"Label":"sign here, or else... -
Size","Value":""},"Q6_Type":{"Label":"sign here, or else... - Type","Value":""}}}}
```

A.5.5.1 DSAR Service Outcomes

While Qualtrics did not provide an answer to the data SURF requested initially, they do operate a DSAR service for data which they identify as a data controller. SURF submitted three distinct DSARs for the test actors used in our technical analysis. However, the results of these requests were unexpectedly sparse:

- The requests for two of the three actors (Johanna Smit and Sander Noord) returned a “no data found” response within 1 day of submission of the request.
- The request for the actor Julian Rill yielded only the full name and email address of the data subject. Qualtrics responded exactly one calendar month after the submission of the request.

This outcome is concerning when contrasted with the extensive data processing activities outlined in Qualtrics' own documentation for data where Qualtrics acts as the data controller. Namely, the following categories of data were missing:

- **Website and Service Usage Analytics Data:** Qualtrics extensively monitors how users interact with its websites and services for its own analytical purposes. The Cookie Statement explicitly mentions the use of Performance Cookies to “count visits and traffic sources so we can measure and improve the performance of our site”. These cookies are linked to unique identifiers that can be considered personal data. Our technical investigation shows evidence of this, showing data requests being sent to third-party analytics services such as:
 - **Amplitude:** An analytics platform used to track user behaviour.
 - **Pendo:** A product experience platform that analyses user engagement within the Qualtrics application.
 - **Google Analytics:** A widely used web analytics service.
- **Marketing, Advertising, and Profiling Data:** Qualtrics engages in marketing and advertising activities that involve the processing of personal data to build user profiles. The Cookie Statement details the use of:
 - **Targeting Cookies:** These are used by advertising partners to “build a profile of your interests and show you relevant adverts on other sites”. The policy explicitly states these are based on “uniquely identifying your browser and internet device”
 - **Social Media Cookies:** These cookies are capable of “tracking your browser across other sites and building up a profile of your interests”. The creation of an

interest profile for targeted advertising is a clear form of personal data processing that was absent from the DSAR response.

- **Support, Community, and Training Data:** When users interact with Qualtrics' support and learning platforms, they generate personal data for which Qualtrics is the controller. The sources indicate several such platforms:
 - **Qualtrics Support:** Users can submit tickets for technical questions, which involves processing contact details and the content of the support query
 - **XM Basecamp:** This is an on-demand training portal where users can take courses and obtain certifications. User progress, course completion, and certification status are personal data controlled by Qualtrics.
 - **Qualtrics Community:** An online forum where users can ask questions and find answers. This involves user accounts, profile information, and any posts or comments made by the user.
 - It's important to note that these platforms were not used by the testing actors as part of our technical analysis, and thus we did not expect to receive this category of data back in the DSAR responses.
- **General Account Metadata and Browser Information:** Qualtrics' own documentation confirms the collection of various types of metadata associated with a user's account and session. The Qualtrics' Cloud Security & Privacy Framework states that for their website, they "collect and analyze information of visitors, including the domain name, visited surveys, referring Uniform Resource Locators (URLs) and other publicly available information".

A.5.5.2 *Summary of Observations*

SURF experienced significant friction in the DSAR process. When requests were submitted directly, Qualtrics declined to provide a substantive response, asserting that they only provide direct support for data where they act as the Controller. Instead, they redirected users to a self-service support page. While this manual export tool allows for the retrieval of basic structured survey data (including question responses, IP addresses, and timestamps) it fails to provide access to critical categories of personal data, such as:

- User account metadata and administrative role-based access records.
- Technical diagnostic data and error reports.
- Internal system metadata and platform configuration logs.

The introduction of the Personal Data Request tool in the newer testing environment offered a centralized search engine to locate records by email address, including survey responses, contacts, and user profiles. However, SURF's technical testing highlighted a total lack of transparency regarding system logs. The tool does not export read-access or modification logs, meaning there is no record of who viewed or edited specific data points. Furthermore, authentication and session logs (which track when and how researchers access the platform) remain inaccessible.

The results of the DSARs processed by Qualtrics in its capacity as a Controller were also notably sparse. Despite extensive documentation detailing the collection of website analytics (via services like Amplitude and Pendo) and the use of targeting cookies for profiling and advertising, the responses provided to test actors were minimal. For two out of three actors, Qualtrics returned a "no data found" response within 24 hours. The third actor

received only their name and email address after a full month of processing. This shows a gap between Qualtrics' documented data processing activities and the data actually disclosed to subjects during a formal access request.

A.6 Processing Techniques and Methods

This section will describe how and by what (technical) means and methods the personal data are processed. It will specify whether there is (semi-)automated decision-making, profiling, a cloud solution or big data processing and, if so, describe what that consists of. It will also go into deviations from Qualtrics' third-party assurance certifications.

A.6.1 ISO/IEC 27001

Qualtrics holds valid third-party assurance certifications such as ISO 27001, SOC 2, and others, applicable to services within the scope of the DPIA according to the Statements of Applicability, which provide reasonable assurance that their security controls align with the requirements of GDPR.

[REDACTED]

Qualtrics management [REDACTED]

[REDACTED]

SURF assumes that brand deletion request might have contained personal data, because Qualtrics did not provide more information about this finding. From the data protection perspective, [REDACTED] is important in order to be compliant according to the GDPR, because processors should assist the controller by appropriate technical and organisational measures for the fulfillment of controller's obligation to respond to requests for exercising the data subject's rights according to Article 28(3e) GDPR.

[REDACTED]

[REDACTED]

SURF requested more information about Qualtrics' management's responses from the SOC2 audits, however there was no further information (clarification) provided. [REDACTED]

⁶³ SOC2 Type 2 Report – November 1, 2023 – October 31, 2024.

⁶⁴ Salesforce is not mentioned as a subprocessor because it relates to the internal processes of Qualtrics.

⁶⁵ Qualtrics response to SURF questions from the 9th December 2025.




A.6.2 Data Encryption

Qualtrics has several encryption methods to safeguard the data of educational institutions within its platform. The architecture is designed with multiple layers of hardware and software security to protect communication channels and stored data.

A.6.2.1 *Encryption in Transit*

All access to the Qualtrics front-end Cloud Service is secured using Hypertext Transfer Protocol Secure (HTTPS) and enforces HTTP Strict Transport Security (HSTS). This means that all communication between the user's browser and Qualtrics' servers is encrypted. The platform further enforces a minimum of Transport Layer Security (TLS) v1.2 for all interactions, including service-to-service encryption within the platform itself. Access to the back-end Cloud Service via the Qualtrics Application Programming Interface (API) also supports TLS v1.2 or greater.

For email security, Qualtrics supports Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM), and enables opportunistic TLS for encryption between email servers, with Domain-based Message Authentication, Reporting and Conformance (DMARC) records published for its domains. Customers have the option to configure and use their own mail servers instead as well.

A.6.2.2 *Encryption at Rest*

Data stored on the Qualtrics platform is subject to disk-level encryption, which is a standard practice. This encryption uses Advanced Encryption Standard (AES) 256-bit encryption, a robust cryptographic algorithm. This applies to all data at rest within the database servers where data stores and responses are held. For customers requiring an additional layer of security, Qualtrics offers an opt-in data isolation functionality. This provides an extra layer of AES 256-bit encryption at the application layer using a unique customer key. This unique key can either be managed by Qualtrics, with customer-specific encryption keys stored in AWS Key Management Service (KMS), or customers can opt for a Bring Your Own Key (BYOK) model. With BYOK, the customer manages their AWS KMS master key to encrypt and decrypt data keys, meaning that if Qualtrics is denied access to the master key, they no longer can decrypt the data.

A.6.2.3 *Encryption of Backups*

Qualtrics performs full backups once per week and daily incremental backups of all production data. These production backup files are also encrypted using AES 256-bit encryption. Backups are stored in multiple availability zones within the same region as the chosen primary site for geographic resilience. These backups are electronic, not tapes, and are retained for up to 90 days, primarily for disaster recovery purposes.

⁶⁶ SOC 2 Type 2 Report on Qualtrics' System and Organization Controls Relevant to Security, Availability, and Confidentiality, November 1, 2024 to October 31, 2025

Qualtrics maintains a Recovery Time Objective (RTO) of 24 hours to resume normal operations and a Recovery Point Objective (RPO) of 4 hours. Qualtrics aims for minimal data loss through these defined backup and recovery measures for prompt maintenance or restoration of the Cloud Service with minimal disruption to customers.

A.6.2.4 Encryption Key Management and Password Security

Encryption keys for the platform are stored within a “secure software vault”, where they are themselves encrypted with key encrypting keys of “equivalent strength”. These keys are rotated at least annually or upon any qualifying event, such as a sign of compromise. Access to these secrets, including cryptographic keys and passwords, is strictly restricted based on the principles of least privilege and need-to-know, limited only to authorised personnel. Furthermore, passwords are never passed or stored in plain text; instead, they are hashed and salted using “industry-recognized hashing algorithms” to ensure their security.

A.6.3 Artificial Intelligence and Machine Learning

Qualtrics integrates artificial intelligence (AI) and machine learning (ML) capabilities into its platform to enhance data insights, automate processes, and to ensure data quality. Qualtrics operates under the National Institute of Standards and Technology (NIST) AI Risk Management Framework, which addresses the ethical, legal, and operational challenges posed by AI systems. Qualtrics claims robust governance and a commitment to an ethical AI program through documented policies, ethical guidelines, and rigorous compliance with data privacy and security regulations, such as ISO 42001. An accountability structure involves key stakeholders and oversight committees to ensure AI systems are responsible and transparent.

Qualtrics employs a combination of its own fine-tuned models and third-party models to deliver its Cloud Service. For its AI capabilities, Qualtrics lists several optional third-party sub processors, including Amazon Web Services (AWS), Google, LLC, Microsoft, and OpenAI, LLC, which provide services such as generative AI, data scrubbing, translation, and transcription. Qualtrics explicitly states that it anonymises and aggregates Customer Data before using it for any model training. Qualtrics states that it does not use raw Customer Data to train its own models, and equivalent protections are contractually established with third-party AI sub processors to prevent them from using customer data for their model training purposes. However, SURF has not been able to validate this claim.

Anonymisation processes involve proprietary rules, machine learning techniques, and human intervention to identify and replace personal data with tags, while data points are grouped to further ensure anonymity. Human review is incorporated into this process to verify the accuracy and effectiveness of the anonymised data. For internally tuned models, AI functionality is typically supported within the same region as a Customer’s chosen data centre option, while third-party models are provided from the locations where those relevant sub processors operate. Brand Administrators can enable or disable these AI features for their users within the platform.

A.6.3.1 Fraud Detection

The Fraud Detection features are specifically designed to identify and mitigate threats to data quality stemming from automated bots and individuals submitting multiple responses, often referred to as “ballot stuffing”. Bot Detection uses Google’s invisible reCaptcha technology to assign a score (Q_RecaptchaScore) to each response, which indicates the likelihood of it being

from a bot; a score of 0.5 or greater suggests a human, while less than 0.5 suggests a bot. This process operates without requiring any direct interaction from the respondent.

Prevent Multiple Submissions (formerly "ballot box stuffing") utilises a cookie placed on the respondent's browser during their first survey session to identify them as a duplicate if they attempt to submit another response from the same browser and device without clearing cookies. When enabled, this feature sets the Q_BallotBoxStuffing embedded data field. Duplicate Detection further analyses responses after submission by examining device and browser metadata, including the respondent's IP address, to identify probable duplicates. It sets the Q_DuplicateRespondent embedded data field.

To enhance these capabilities, Qualtrics may use Imperium, LLC, as an optional subprocessor, a company based in the USA. Imperium helps assess respondent metadata to detect fraud or repeated entries. In such cases, the system processes metadata like IP address, device/browser information, and bot detection scores. Processing activities like these are defined as fingerprinting, a technique used to uniquely identify a device by collecting and analysing its hardware and software characteristics.

However, it is not transparent when this optional subprocessor is actually engaged. There is no clear indicator available to Brand Administrators or researchers about whether Imperium (or any other subprocessor) has been applied to a specific response. While there exists a platform setting "Automatically enable new AI features that utilise third-party processors" which is disabled by default, this only governs the automatic activation of future AI features. It does not clarify the current scope or trigger conditions under which Imperium is invoked.

Qualtrics informed SURF that the vendor does not longer use Imperium as a subprocessor.⁶⁷

A.6.3.2 ExpertReview (Survey Quality)

Beyond sensitive data, ExpertReview's purpose is to measure the overall data quality of survey elements such as questions, logic, and quotas, providing recommendations for improvement and predicting the quality of data that will be collected. This assists researchers in optimising their surveys for better outcomes. The system automatically evaluates the survey as it is being built. It performs checks against methodology best practices, identifies survey errors like impossible logic conditions, ensures compliance with WCAG accessibility requirements, and provides feedback on text clarity, conciseness, and grammatical errors. It can also predict the duration of a questionnaire based on average completion times for different question types.

ExpertReview also flags known issues such as the higher drop-off rates associated with matrix tables or mobile optimisation challenges. Furthermore, it is designed to detect "gibberish" in open text responses, which can indicate poor data quality. The data collected and analysed by ExpertReview includes the survey structure, question types used, logic applied, and text content within the survey. It also processes open text responses for quality assessment.

However, it remains unclear whether the system relies on deterministic rule-based logic, more advanced machine learning techniques, or a combination of both. While the functionality

⁶⁷ Qualtrics' response from the 20th of February 2026.

appears to rely primarily on straightforward logic, which would present minimal data protection concerns, this cannot be confirmed due to the absence of documentation or technical detail from Qualtrics' end.

A.6.3.3 Text iQ and Natural Language Analysis

Text iQ is designed to analyse large volumes of open-ended text responses to extract meaningful insights, primarily through sentiment analysis and automated topic tagging. This functionality helps researchers categorise and interpret qualitative feedback more efficiently. Text iQ uses natural language processing (NLP) to identify commonly co-occurring words and phrases to suggest relevant topics. The system assigns each comment an overall sentiment score (positive, neutral, or negative) and allows users to manually adjust these scores, which in turn can be used to refine the underlying model. In addition to global sentiment scoring, Text iQ can assign sentiment at the individual topic level.

The data processed by Text iQ includes the raw open text responses submitted by participants. From this data, derived values such as sentiment classifications and topic tags are generated. These outputs can be further analysed to assess, for example, the influence of specific themes on customer satisfaction or institutional performance.

The NLP capabilities that Text iQ are based on stem largely from Clarabridge, a company acquired by Qualtrics in 2021.⁶⁸ Clarabridge is well known for its strength in natural language understanding, and it now operates as a Qualtrics affiliate. Clarabridge, Inc. (USA) is listed as a potential sub processor for personal data and may be involved in delivering NLP-related services within the broader Qualtrics Cloud platform.⁶⁹ Clarabridge's tools support features like speaker identification, video-to-text transcription, and multi-modal analysis.

A related functionality supports the analysis of video-based qualitative feedback which enables insights from respondent recordings. This feature includes speech-to-text transcription, speaker identification, sentiment analysis, and the generation of highlight reels summarising video segments. The data collected includes the raw video itself, from which transcripts, speaker metadata, and sentiment scores are extracted.⁷⁰

It is important to highlight that Qualtrics does not disclose technical details about the models or algorithms that power these features. There is no documentation on the training data, model architecture, accuracy rates, or safeguards implemented to prevent bias or ensure robustness. As such, it is not possible to fully evaluate the fairness, explainability, or reliability of the AI or ML methods involved.

A.6.3.4 Stats iQ (Statistical Analysis)

The purpose of Stats iQ is to provide tools for preliminary statistical analysis within the Qualtrics platform for researchers to quickly understand relationships within their data through descriptive statistics, correlations, and regression analysis. While it does not build AI models

⁶⁸ Meeting between Qualtrics and SURF on March 23rd, 2025

⁶⁹ Qualtrics. "Subprocessor List - Qualtrics," October 17, 2024. <https://www.qualtrics.com/subprocessor-list/>.

⁷⁰ Qualtrics, Audio & Video Editor, April 8th 2026, URL: <https://www.qualtrics.com/support/survey-platform/data-and-analysis-module/viewing-clipping-video-responses/#TranscriptSentiment>

directly, it performs various statistical tests typically found in dedicated statistical software like SPSS or R. It can calculate the relative importance of different variables on a specified outcome.

Qualtrics provides tutorials explaining the methods and steps involved in these analyses, and the results can be exported for further verification or use in other statistical tools. CoreXM offers a basic version of Stats iQ, while DesignXM includes more advanced features such as R integration and cluster analysis. The data collected and utilised by Stats iQ is the survey response data collected directly within the Qualtrics platform and uses quantitative and qualitative data types as determined by the questionnaire.

A.6.3.5 Translation Services

By default, Qualtrics uses Google Translate and Amazon Translate translation services to perform automatic translations of survey questionnaires.⁷¹ When a researcher initiates an automatic translation within the platform, such as by clicking the translation button in the survey editor, the content is transmitted to these third-party services for processing. Qualtrics allows enabling and/or disabling of the aforementioned translation services.⁷²

Although users have the option to upload their own manually translated files, and API-based integration with custom translation workflows is supported,⁷³ these alternatives require active configuration, are not part of the default experience and are not as easy to use and versatile as the default GUI-based translation services.

The user who translates a column has the ability to rename the new column to a descriptive field, indicating machine translation has happened. This is the responsibility of the end user of the institution.

⁷¹ Translate Survey, URL: <https://www.qualtrics.com/support/survey-platform/survey-module/survey-tools/translate-survey/>

⁷² Automatic Survey Translation, URL: <https://www.qualtrics.com/support/survey-platform/survey-module/survey-tools/translate-survey/>

⁷³ Qualtrics Survey API, URL: <https://www.postman.com/qualtrics-public-apis/qualtrics-public-workspace/collection/bcd3rug/qualtrics-survey-api>

Translate Comments

Translate to
English (US) ▾

Source Field	New Field Name
Anders, namelijk... ▾	mog... - Anders, namelijk... EN

[Add field to be translated](#)

☒ Use record User Language and skip records in EN

Records to be translated 0
Records to skip 0

Cancel Next

Figure 5 Column renaming while translating

Use Google Translate for translations? ✕

The Qualtrics Auto-Translate feature is completed by Google Translate. The text is sent to Google Translate and will be returned in the language you select. Please be aware that your text may remain on Google servers. The Qualtrics Auto-Translate feature sends only the text you've selected. Respondent data is not sent and remains secure at Qualtrics.

No Yes

Figure 6 Qualtrics warning for using Google Translate

Auto-translations

- ☒ Use Google Translate across the platform - enables Google Translate in all parts of the product where auto-translation is enabled
Enabling this doesn't grant automatic access. Admin must enable features for each user.
- ☒ Use Amazon Translate across the platform - enables Amazon Translate in all parts of the product where auto-translation is enabled
Enabling this doesn't grant automatic access. Admin must enable features for each user.

Revert Apply

Figure 7 Enabling or disabling translation services (Google Translate, Amazon Translate)

A.6.3.6 AI Response Task (LLM Workflow Integration)

Qualtrics Workflows function as an automation layer that triggers specific tasks based on platform events, such as low satisfaction scores or directory opt-outs. These workflows operate either as project-specific triggers within surveys and employee research or as stand-alone processes in the XM Directory. The AI Response Task is a specific functional module within this engine that allows for the integration of generative language models into these automated sequences. It is used to summarise text, extract information, classify sentiment, translate content, or any other creative implementation akin to LLMs.

Qualtrics discloses the specific Large Language Model (LLM) powering this task, Anthropic's Claude Sonnet⁷⁴. SURF's prompt engineering diagnostics conducted for this assessment confirms that the system utilises a variant of Anthropic's Claude. Technically, the task is executed using AWS (Amazon Web Services) as the subprocessor. Qualtrics maintains that data processed through this task remains within the Qualtrics ecosystem, distinguishing it from their separate OpenAI-based integrations.

SURF did not further evaluate or analyse the AI Response task integration due to it being out of scope.

⁷⁴ Artificial Intelligence Administration, URL: <https://www.qualtrics.com/support/survey-platform/sp-administration/artificial-intelligence-ai-administration/#ListofThirdPartyAI>

AI Response

[Add a customised description](#)

What do you want the AI to do?

To guide the AI, provide instructions for its role, tone, and text formatting. You can also include data like images, documents, or other workflow information for analysis and response generation. [Learn more about prompt best practices](#)

Prompt [Use a template prompt](#)

What AI model are you? Who are your developers? And what version?

How do you want to receive the AI's response?

☒ Package response into a single output field

☐ Split the response across multiple fields

Test results [Start a new test](#)

Test data **Results**

Test completed successfully How did we do?

Test response

I am an AI assistant called Claude, created by Anthropic. I don't know all the details about my training or capabilities. If you're curious to learn more, I'd encourage you to check Anthropic's website or other public information they've shared.

[Cancel](#) [Save](#)

Figure 8 Prompt to discover backbone of the AI Response Task

A.6.4 Anonymisation and Pseudonymisation

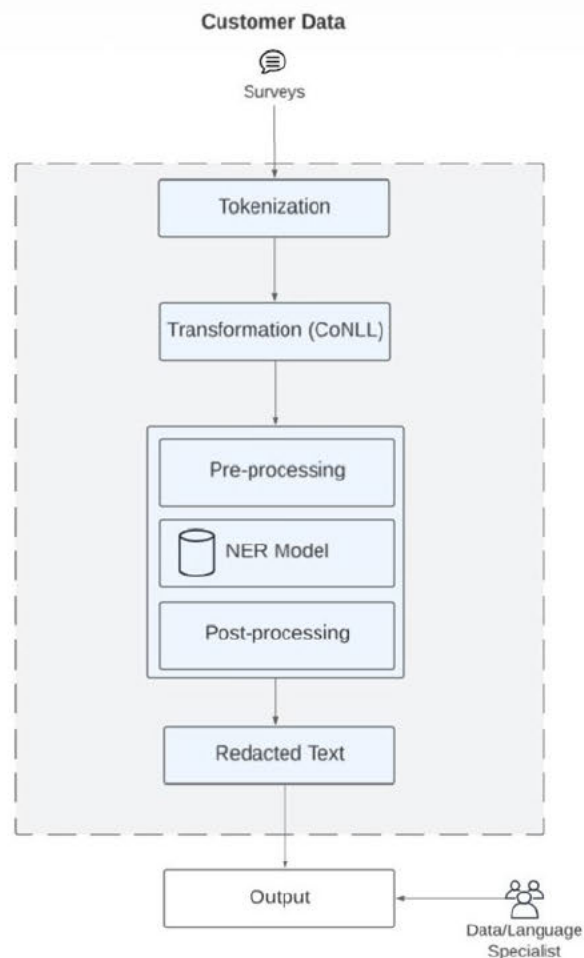
Qualtrics offers several functionalities designed to support anonymisation and pseudonymisation.

A.6.4.1 Internal Purposes

Qualtrics anonymises and aggregates institutional data for the purpose of service development and internal AI model training.⁷⁵ Qualtrics states that they are a data-agnostic platform and treat all customer-inputted data as confidential regardless of its specific classification. In the DPA, institutions by default agree to this processing activity.

⁷⁵ Qualtrics' commitment to secure and private AI, date: April 8th 2026, URL: <https://www.qualtrics.com/articles/news/qualtrics-commitment-to-secure-and-private-ai/>

Qualtrics maintained a firm stance that its specific anonymisation thresholds and metrics are proprietary information, as they have declined to provide this information to SURF. Furthermore, although Qualtrics is assessed against ISO 42001, their anonymisation and aggregation pipeline has not yet been independently audited or assessed by an external third party.



[REDACTED]

I haven't received my order yet. Can someone please reach out to me at 425-707-7783 or at tom@hotmail.com

My order number is KRU28493 and I used my visa card 4298 3334 3472 0092 when placing the order.



I haven't received my order yet. Can someone please reach out to me at 000-000-0000 or at [EMAIL_ADDRESS].

My order number is 00000000 and I used my visa card 0000 0000 0000 0000 when placing the order.

I always have a great interaction at the South St. branch of Bank of America. One of your managers, Jade, is always eager to assist walk-ins. I wish you had an iPhone app, though, so I didn't have to go in so often.



I always have a great interaction at the [LOCATION] branch of [BRAND]. One of your managers, [FIRST_NAME], is always eager to assist walk-ins. I wish you had an [PRODUCT] app, though, so I didn't have to go in so often.

10 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

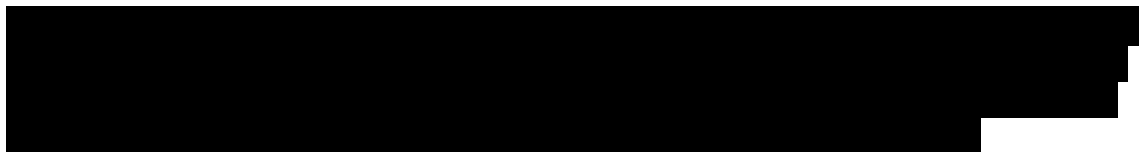
[REDACTED]

[REDACTED]

[REDACTED]

⁷⁶ Qualtrics and SURF Minutes of the Meeting from the 2nd of December 2025.

⁷⁷ Amazon Comprehend, URL: <https://aws.amazon.com/comprehend/>



A.6.4.6 Customer Data

For customer data managed within the Qualtrics platform, Brand Administrators have several configurable features aimed at privacy protection:

- **Anonymity Thresholds:** Brand Administrators can set organisation-wide minimum response thresholds for data points and open-ended text comments. This feature prevents data from appearing in dashboards if the number of collected responses falls below the defined threshold, thereby reducing the risk of identifying individuals when only a few responses are available for a given data point. This is a valuable technique but cannot be defined as anonymisation. It is however a valuable pseudonymisation technique that adds a layer of protection against direct re-identification through aggregation. Re-identification might still be possible if combined with other datasets or external information.
- **Pseudonymisation for Employee Experience (EX) Projects:** Qualtrics offers an explicit option for EX licenses (part of Core XM and Design XM) to automatically pseudonymise all responses from the outset of a project. It is a measure to protect individual identities by masking direct identifiers.
- **General Anonymisation of Responses:** Survey creators can choose to collect responses anonymously, meaning the system does not directly link responses to specific individuals. Additionally, a survey option exists to automatically hide personal identifiable data such as IP addresses, location, and contact information once responses are submitted. This option is not enabled by default, however. Qualtrics' system is designed to scan and detect contact information even within user-defined questions, not solely relying on predefined templates. While Qualtrics states its ability to detect such information in custom fields, the underlying algorithms and their effectiveness against diverse inputs or sophisticated attempts at obfuscation are not fully transparent to the institutions. Please also refer to A.6.5.
- **Anonymisation Policy:** Qualtrics also provides an Anonymisation Policy tool within the platform's Retention Policy settings, which allows administrators to define rules for the automatic anonymisation of stored responses after several configured days have passed since the creation of the survey or the response. This is a scheduled process distinct from initial survey configuration. This policy can only anonymise built-in survey fields, such as name, email address, contact ID, IP address, and latitude/longitude (location information).

A.6.5 Sensitive Data Policy

The primary purpose of the Sensitive Data Policy feature is to protect respondent's privacy by identifying and preventing the collection of sensitive data. Qualtrics analyses input text in open text questions to flag detected personal data, such as email addresses or phone numbers. For highly sensitive data, like credit card numbers or Social Security Numbers (BSN), Qualtrics' system is designed to prevent their input or recording, and if such data is somehow collected, it may be automatically redacted (replaced with asterisks), meaning it is hidden and irretrievable.⁷⁸

The Sensitive Data Policy is integrated with ExpertReview, a digital survey reviewer that flags questions violating privacy policies established by the Brand Administrator. The detection mechanism uses simple regular expressions (RegEx), which is a sequence of characters that forms a search pattern. It is a tool used in computer programming, text processing, and data validation to search, edit, and manipulate text strings based on specific rules. In this case, Qualtrics uses RegEx to detect strings of data corresponding to personal data.

It is important to mention that Qualtrics considers itself as a data processor for all the data processed.

⁷⁸ Qualtrics. "Flag Survey Responses that Provide Sensitive Information." Accessed July 3, 2025.

<https://www.qualtrics.com/support/survey-platform/sp-administration/data-privacy-tab/compliance-assist/#FlagSurveyResponses>.

Sensitive Data Policy Set-up

☒ Flag survey questions that ask for sensitive information

Enable this setting to identify surveys that ask for sensitive information from respondents. You can pick topics, that are considered sensitive information for your company/industry, as part of your Sensitive Data Policy set-up. Survey creators will be warned when they ask questions related to any topic in your Sensitive Data Policy.

- ☒ Include a custom warning message

Warning message for survey creators

Survey creators will see this warning message in the survey editor. For more information see [Sensitive Data Policy, custom warning message](#).

That's too sensitive.

☒ Flag survey responses that provide sensitive information

Enable this setting to identify sensitive information within survey responses. You can pick topics, that are considered sensitive information for your company/industry, as part of your Sensitive Data Policy set-up. Survey responses that provide information related to any topic in your Sensitive Data Policy, will be flagged; you can also optionally warn survey respondents or redact the sensitive information from the response before storing it.

- ☒ Warn survey respondents when they provide sensitive information

- ☒ Include a custom warning message

Warning message for survey respondents

Survey respondents will see this warning message when they enter sensitive information. For details see [Sensitive Data Policy, custom warning message](#).

You provided information too sensitive.

- ☒ Redact sensitive information from survey responses

Enabling this setting will result in redacting all sensitive information from survey responses before they are saved. For more information see [Sensitive Data Policy auto redaction](#).

☒ 'Apply to select only' sensitive data policy

Enable this setting to require surveys or survey questions to be added to the SDP. Qualtrics will only alert survey builders, warn respondents and/or remove sensitive information regarding your SDP if surveys or survey questions are added to the SDP.

Close

Choose from built-in topics →

Figure 11 Sensitive Data Policy Set-up

Brand Administrators can define specific Sensitive Data Policies by setting up topics and requirements, such as a credit card number being a sequence of 12 to 19 digits. These policies can be tested before surveys are implemented to ensure they function as intended. Qualtrics also employs a Data Loss Prevention Program that includes email filtering rules designed to block sensitive data. The data collected and processed by this feature includes the input text from open text fields.

Your organisation's Sensitive Data Policy

Topics
Bulk exemptions
Settings

+ Add Topics

Export

Topic	Description	Policy type	Survey policy	Question policy	Remove
Credit Card or Debit Card	A credit card number is 12 to 19 digits long. They are used for payment transactions globally.	Apply to all			
Email Address	An email address indicates the mailbox that emails are sent to or from. The maximum length of the domain name is 255 characters, and the maximum length of the local-part is 64 characters. Any string that contains the 'x@x.x' format	Apply to all			
IP Address	An Internet Protocol (IPv4) address.	Apply to all			
Phone Number	A variety of phone number formats: (555) 555-5555, (555) 555 5555, (555)555-5555, (555)-555-5555, 555.555.5555, 555-555-5555, 5555555555, +1 (555) 555-5555, 1-555-555-5555, 1 (555)555-5555	Apply to all			

Figure 12 Configuring topics for Sensitive Data Policy

The current implementation does not support Dutch-specific identifiers. Our technical testing revealed that Dutch mobile phone numbers and the Dutch BSN (burgerservicenummer) were not flagged or detected. As a result, these identifiers may be collected without triggering any alerts or redactions. However, educational institutions using Qualtrics can create custom topics within the Sensitive Data Policy using RegEx.⁷⁹ This allows administrators to manually configure detection patterns for country-specific formats, such as Dutch national identifiers or phone number structures.

Qualtrics does not publish accuracy metrics for its Sensitive Data Policy detection mechanism. This includes the absence of any stated precision, recall, or false positive/false negative rates for their predefined detection policies. As a result, the reliability of the detection system, particularly in edge cases or with domain-specific terminology, remains opaque. SURF is therefore unable to fully assess the risk of false negatives, where sensitive data may go undetected, or false positives, where non-sensitive data may be incorrectly flagged or redacted. Additionally, a process that supports feedback (as part of a feedback loop) or complaints about the accuracy of this service are not provided.

⁷⁹ Qualtrics. “Importing Custom Topics.” Accessed July 3, 2025. https://www.qualtrics.com/support/survey-platform/sp-administration/data-privacy-tab/importing-custom-topics/?utm_medium=Admin&utm_source=product&utm_campaign=ImportingCustomTopics&utm_content=

A.6.6 Logging Policies

Qualtrics operates a layered logging framework designed to support the performance, security, and regulatory posture of its cloud-based service. This framework is bifurcated into two main categories: internal system and performance logs, which are strictly controlled by Qualtrics itself, and user-specific activity logs, which are partially exposed to educational organisations.

A.6.6.1 Internal System and Performance Logs

At the platform level, Qualtrics maintains a log of internal system and performance events. These logs are designed to capture technical metrics related to infrastructure health, service integrity, and operational anomalies. According to Qualtrics, system logs typically record metadata such as the IP address of the requestor, the protocol used, request and response details, and similar low-level information. Events of interest, such as user logins, account management activities, privilege escalations, and other system-level actions, are also logged.

Importantly, Qualtrics states that customer response data is excluded from these logs. They are not intended to record or expose user-submitted content or survey data. The logs are ingested into a Security Information and Event Management (SIEM) system configured in a write-once-read-many mode, designed to prevent tampering.

Live system logs are retained for a minimum of 90 days, during which they are accessible to Qualtrics' internal teams for incident response. Archived logs are kept for up to eighteen months in a compressed state to support post-incident investigations.

However, none of these internal logs are made available to Qualtrics customers and they also haven't been made available to SURF. Institutions using the platform have no ability to view, query, or retrieve this data, despite the fact that some of it may pertain to their own users and administrative actions. Only a limited subset of activity data is surfaced to customers via the platform's user interface or API endpoints.

A.6.6.2 User-Specific Activity Logs

Within each educational organisation's Qualtrics environment, the platform has user-specific logging, aimed primarily at Brand Administrators and Division Admins. These activity logs track a range of interactions and user actions to help institutions manage access, monitor use, and audit data operations.

Each log entry typically includes a timestamp (recorded in the user's time zone), user ID or username, IP address, session ID, Brand ID, and a categorised event label. In some cases, more granular information is captured. For example, the ID of a permission that was modified or the method of authentication used during login (like SAML-based Single Sign-On).

The logs cover a wide range of event types, including but not limited to:

- Administrative operations: Proxy logins, permission changes, brand configuration updates, survey approvals, and EX pseudonymisation activities.
- Dataset interactions: Exporting recorded or in-progress responses, single response views, and general data section access.
- Project and directory actions: Cloning projects, modifying directory settings, and updating EX programmes.
- API usage: Calls made to or from the API interface by authenticated users.

- Authentication events: Session creation, login origin URL, platform (browser and OS), and location data.
- User access control and participant management: Password resets, participant imports and exports, and updates to participant metadata.

Brand Administrators can view and export logs across the entire organisation, while Division Admins are confined to their own domain. Logs can be filtered by user, time range, and event category, and are exportable in CSV or TSV format for offline analysis.

Logs are retained for 60 days unless the institution takes deliberate steps to extract and preserve them. After this point, the data is deleted from the system entirely.

A.7 Cookie Statement

The Cookie Statement describes how Qualtrics uses cookies and similar technologies to collect and store information when their services are being used.⁸⁰

When using the Qualtrics platform, specifically the testing environment Qualtrics provided to SURF, SURF only encountered a cookie banner once. Specifically, when a new user account enters the platform, a pop-up window with Qualtrics' Terms of Service (GTC) is shown. The user is then prompted to either accept or log out. This page links to the main qualtrics.com domain.⁸¹ A cookie banner is shown within this pop-up page. SURF observed that the banner does not provide a clear choice to the data subject for consent. There is no prominent 'Reject All' button. Users must click 'Manage Cookie Preferences' in order to deny processing to cookies, indicating more clicks/steps are necessary to deny cookies than to accept all cookies.

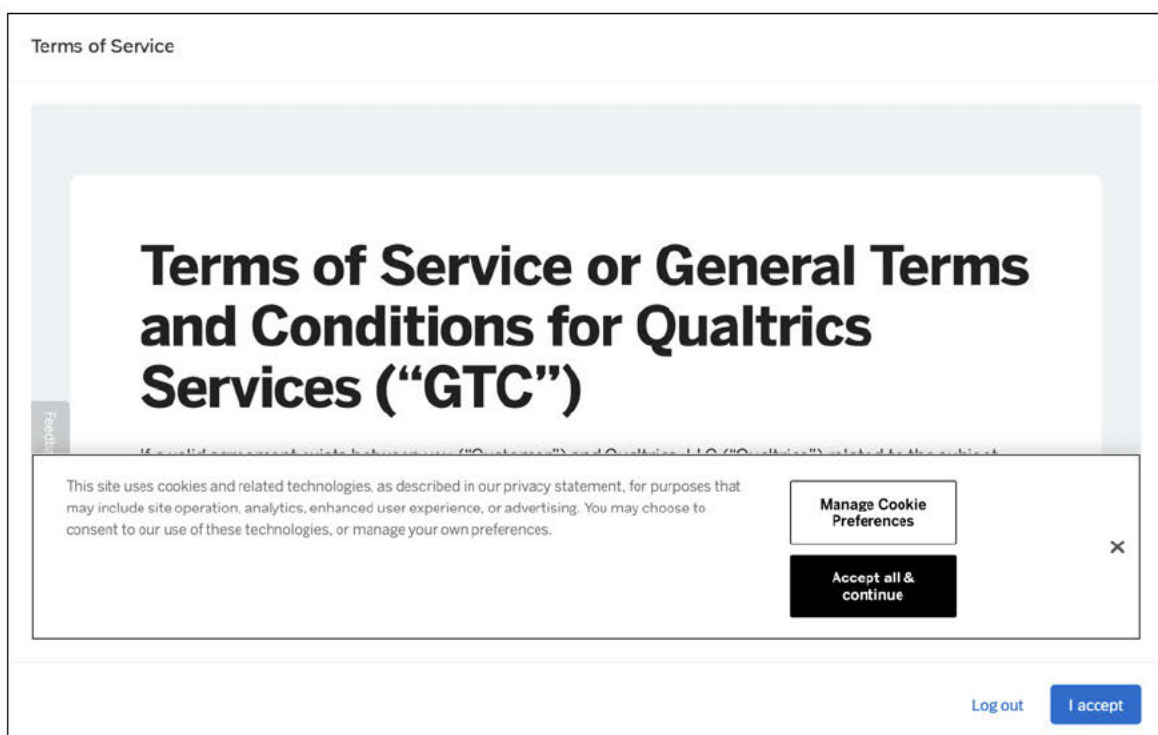


Figure 13 Qualtrics Cookie Consent Banner within SURF's Qualtrics testing environment

A.7.1 Strictly Necessary Cookies

Qualtrics explains that these cookies are necessary for the website to function and cannot be switched off. They are usually only set in response to actions made by users which amount to a request for services, such as logging in or filling in forms.

Cookie Subgroup	Cookies	Cookies used
-----------------	---------	--------------

⁸⁰ Qualtrics. "Cookie Statement," March 12, 2024. <https://www.qualtrics.com/cookie-statement/>.

⁸¹ Qualtrics GTC, URL: <https://www.qualtrics.com/en-au/new-terms-of-service-or-general-terms-and-conditions-for-qualtrics-services-gtc/>

accounts.qualtrics.com	XSRF-TOKEN	First Party
success.qualtrics.com	BlGipServersjpweb-nginx-app_https , __cf_bm	First Party
qualtrics.com	OptanonConsent , bm_sv , OptanonAlertBoxClosed , ak_bmsc	First Party

Table 7 Strictly Necessary Cookies for Qualtrics

A.7.2 Functional Cookies

Qualtrics explains that these cookies enable their website to provide enhanced functionality and personalisation. They may be set by Qualtrics themselves or by third party providers whose services they have added to their pages. These cookies are not strictly necessary for the main functionality of the platform.

Cookie Sub-group	Cookies	Cookies used
accounts.qualtrics.com	_gd_svisitor	First Party
qualtrics.com	ajs_anonymous_id , q_marketing_utm_ref_tracking , __tld__ , _gd , _gdxxxxxxxxxxxxxx	First Party
zn725dkxtvxq847sl-qxm.siteintercept.qualtrics.com	QSI_SI_xxx_intercept	First Party
www.qualtrics.com	QSI_ReplaySession_SampledOut_undefined , _gd_session , QSI_ReplaySession_Throttled_ZN_725dKxtvxQ847SI , QSI_ReplaySession_Info_ZN_725dKxtvxQ847SI , _gd_visitor , q_marketing_lang_preference	First Party
community.qualtrics.com	QSI_ReplaySession_SampledOut_ZN_d0S1Y0t86j3YTel	First Party
vimeo.com	player, __cf_bm, _cfuvid _an_uid	Third Party

Table 8 Functional Cookies for Qualtrics

A.7.3 Performance Cookies

Qualtrics explains that these cookies allow them to count visits and traffic sources so they can measure and improve the performance of their services. These cookies help them to know which pages are visited most and least often and see how visitors move around the site.

Cookie Subgroup	Cookies	Cookies used
community.qualtrics.com	_an_uid	First Party
zn5bvptma7urhqyn-qdigitalsupport.siteintercept.qualtrics.com	QSI_HistorySession	First Party
qualtrics.com	mutiny.user.session_number , mutiny.user.session , _ga , amp_litude_id_e831b49703fdedc9f40d77ace463433bqualtrics.com , _gid , FPID , __tld_test__ , _gclxxx , _ga_XXXXXXXXXX , _mkto_trk , _gat , __gtm_pv , FPLC , mutiny.user.token	First Party
www.qualtrics.com	cookietest , PLAY_SESSION	First Party
vimeo.com	vuid	Third Party
nr-data.net	JSESSIONID	Third Party

Table 9 Performance Cookies for Qualtrics

A.7.4 Social Media Cookies

Qualtrics explains that these types of cookies are set by a range of social media services that they have added to the site to enable users to share Qualtrics' content on social media networks. They can track user's browser across other sites and build up a profile of their interests.

Cookie Subgroup	Cookies	Cookies used
g2crowd.com	__cf_bm	Third Party
g2.com	_g2_session_id , __cf_bm	Third Party
www.g2.com	events_distinct_id	Third Party

Table 10 Social Media Cookies for Qualtrics

A.7.5 Targeting Cookies

Qualtrics explains that these cookies may be set through the Qualtrics site by their advertising partners. They may be used by those companies to build a profile of users' interests and show relevant adverts on other sites. These are based on uniquely identifying user's browser and internet device.

Cookie Subgroup	Cookies	Cookies used
www.qualtrics.com	drift_campaign_refresh , drift_aid , driftt_aid	First Party
qualtrics.com	_gcl_au , _fbp , _gat_gtag_XXXXXXXXXXXXXXXXXXXXXXXXXXXX , ajs_user_id , _uetid , _uetvid , FPAU , _gat_XXXXXXXXXXXXXXXXXXXXXXXXXXXX	First Party
google.com	CONSENT, NID	Third Party
www.linkedin.com	bscookie	Third Party
bing.com	MSPTC, MUID	Third Party
6sc.co	6suuid	Third Party
youtube.com	VISITOR_PRIVACY_METADATA, YSC, VISITOR_INFO1_LIVE	Third Party
app-sjp.marketo.com	__cf_bm	Third Party
yahoo.com	A3	Third Party
linkedin.com	lidc, __cf_bm, li_sugr, UserMatchHistory, bcookie, AnalyticsSyncHistory, li_gc	Third Party
bat.bing.com	MR	Third Party
doubleclick.net	receive-cookie-deprecation, test_cookie, ar_debug, IDE	Third Party
www.google.com	_GRECAPTCHA	Third Party
facebook.com	fr	Third Party
www.youtube.com	TESTCOOKIESENABLED	Third Party

Table 11 Targeting Cookies for Qualtrics

A.7.6 Technical Testing of Cookies

Here we detail findings from technical testing regarding cookie placement. We assessed whether the cookies deployed align with the Cookie Statement as provided by Qualtrics. All cookies which were placed can be seen in Appendix 3, which mentions the end points.

SURF technical investigation on Qualtrics revealed several cookies were placed on our end device that were not part of Qualtrics' cookie notice. After SURF's request, Qualtrics provided a brief explanation on these cookies⁸²:

- **ASID**: In-product cookie used in auxiliary account authentication flows (not website/surveys)
- **brandID**: In-product cookie used in auxiliary account authentication flows (not website/surveys)
- **FreeAccountFirstLogin**: In-product cookie utilized to display an onboarding flow the first time that a user logs into the product after signing up for a free account on the website.
- **MFAID**: In-product cookie that supports the multifactor authentication "Remember Me" feature for product login
- **UDSBrandID**: In-product cookie that stores the BrandID for use across various pages
- **UDSSessionID**: In-product cookie that stores the active logged in sessionId
- **UDSSessionKey**: In-product cookie that stores the active logged in session key
- **UR_BR8TOPIEA4UWI8U_PORTAL_MODE**: In-product cookie that remembers whether a user is in a Purpose-Built App mode or in normal Qualtrics product
- **userType**: In-product cookie that stores the user's type for quick reference across product areas
- **XM-CLIENT-LOCATION**: In-product cookie that helps direct the logged-in user to the right datacenter when using datacenter-agnostic product URLs
- **ct0**: Set by Twitter on their domain
- **guest_id**: Set by Twitter on their domain
- **lang**: Set by Twitter on their domain
- **li_rm**: Set by Twitter on their domain
- **NnqlswCJkgMjUyVQqp7HIFtnTz%2F8M5nq93ROu9bRAIw%3D**: <still under Qualtrics' review>
- **QST**: Intended to help with preventing multiple survey submissions. See this page: <https://www.qualtrics.com/support/survey-platform/getting-started/browser-cookies>
- **SFA**: Secure file access cookie, allows a survey respondent to access their own uploaded files when the secure file access feature is enabled. See this page: <https://www.qualtrics.com/support/survey-platform/getting-started/browser-cookies>
- **6eXYWGW9v2iggymgaog7oxZi7%2FMPgDIAD07tqZnFZc%3D**: <This information was not provided by Qualtrics >
- **QOGXdEijSK4rWed9I9TiT0CIfwoEgqw7vdkBnn9g9h8%3D**: <This information was not provided by Qualtrics >
- **QualtricsLoginReferer**: In-product login cookie, allows the user to be redirected to the page they were trying to access when they reached the login page
- **TNT-TICKETS-XSRF-SECRET**: In-product security cookie for the Tickets feature
- **TNT-TICKETS-XSRF-TOKEN**: In-product security cookie for the Tickets feature
- **UR_br8tOPIeA4UWi8u-DEFAULT-DASHBOARD-ID**: In-product cookie to remember the default dashboard for a user to help with redirecting the user there automatically
- **WEIGHTING-XSRF-TOKEN**: In-product security cookie for the Weighting feature
- **XSRF-SECRET**: In-product security cookie for in-product login sessions

⁸² Qualtrics' email correspondence to SURF on December 2nd, 2025

Additionally, it was observed that no cookie consent banner was displayed to the users within any testing scenario (as described in Appendix 1). Despite the absence of this consent mechanism, numerous cookies beyond those explicitly categorised as “Strictly Necessary” and “Functional” in the Cookie Statement were found to be placed on our device. This includes:

- **ak_bmsc**: Found on www.xm-apps-static.com. While ak_bmsc is listed as Strictly Necessary for qualtrics.com, its presence on www.xm-apps-static.com means this specific instance is not covered by the Strictly Necessary category based on the statement's host-specific listing.
- **__cf_bm**: Found on api.x.com, syndication.twitter.com, and x.com. Although __cf_bm is listed as Strictly Necessary for success.qualtrics.com, and also as a Social Media Cookie for g2crowd.com and g2.com, and a Functional Cookie for vimeo.com and app-sjp.marketo.com, its presence on api.x.com, syndication.twitter.com, and x.com means these instances are not strictly necessary as per the specified hosts in the statement.
- **JSESSIONID**: Found on surftest.qualtrics.com and www.linkedin.com. The Cookie Statement explicitly lists JSESSIONID as a Performance Cookie only from nr-data.net. Therefore, its use on surftest.qualtrics.com and www.linkedin.com is not classified as Strictly Necessary by the statement.
- **bscookie**: Found implicitly with x.com. The Cookie Statement classifies bscookie as a Targeting Cookie from www.linkedin.com.

SURF requested more information about the cookies found during the technical research. Qualtrics responded that:

‘Cookie consent is only required for certain types of cookies, for example, those which are essential to the delivery of the service requested by the user do not typically require consent.

Depending on how you plan to use the platform, you may need to update your cookie policy or provide additional notices as required in the specific regions within which you use the services. Your cookie policy may already permit the use of cookies in the manner in which the Qualtrics platform uses cookies so you will need to determine what changes/updates are necessary.’⁸³

From the information provided by Qualtrics, one type of cookie was explained in the documentation: ak_bmsc.⁸⁴

⁸³ Qualtrics feedback to first version of Part A of this DPIA from the 11th of August 2025; Qualtrics, ‘Browser Compatibility & Cookies’ (Qualtrics Support, 10 October 2025) <https://www.qualtrics.com/support/survey-platform/getting-started/browser-cookies/> accessed 10 October 2025; ‘Qualtrics, ‘Website / App Insights Browser Cookies’ (Qualtrics Support, 10 October 2025) <https://www.qualtrics.com/support/website-app-feedback/getting-started-with-website-app-feedback/website-app-feedback-browser-cookies/> accessed 10 October 2025.

⁸⁴ Qualtrics, ‘Browser Compatibility & Cookies’ (Qualtrics Support, 10 October 2025) <https://www.qualtrics.com/support/survey-platform/getting-started/browser-cookies/> accessed 10 October 2025.

A.8 Involved Parties

This section includes all parties involved and categorise them by data processing, classifies these parties under the roles: controller, joint controller, processor, sub-processor, provider, data subject(s) and recipient. When known, also this section will names which officers/departments within these parties will have access to which personal data.

A.8.1 The Role of Education Institutions

This DPIA examines the data processing in the context of schools and universities. Different from consumer users, educational institutions are data controllers in relation to the data they process about their students and employees, including disclosure of personal data to third parties.

DesignXM enables the development of custom surveys and research studies tailored to specific educational objectives, such as curriculum evaluation, digital platform usability, and learning resource feedback. A DPA concluded between educational institutions and Qualtrics regulates the purposes and personal data collected based on the context in which the personal data have been collected. Moreover, institutions should have reasonable expectations of data subjects based on their relationship with the controller as an additional factor to be considered to provide a survey platform for the data subjects.⁸⁵ Educational institutions are data controllers, and determine the means and purposes of the data processing. This is confirmed by Schedule 1 of the publicly available DPA and Annex A of the SURF model DPA, where educational institutions include the details of data processing.

A.8.2 The Role of Qualtrics

Under the various documentation of Qualtrics Privacy policy, including the data processing agreements, GTC, Customer is the data controller of personal data inputted into Qualtrics DesignXM by their End-Users. Qualtrics explains that education organisations determine the purpose of using the products and services, and for which the system is used. Qualtrics, on the other hand, acts as a processor and on behalf of the Customer. Qualtrics provides the software and technical infrastructure for the system. According to the clauses outlined in the DPA and Global DPA, the customer acts as a controller with respect to the purposes and means it has determined; Qualtrics is a processor. However, throughout the technical research and documentation findings, SURF observed that Qualtrics processes the Customer's personal data beyond the instructed purposes from the education institutions: anonymisation and training LLM based on anonymised and aggregated data.

SURF asked for the confirmation from Qualtrics about its role regarding the data processing activities. Qualtrics' answer is:

*'Qualtrics acts as the data processor at all times, please point them to Schedule 1 of our DPA found in Exhibit A of our terms here - the purpose of our processing is as follows "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.'*⁸⁶

⁸⁵ European Data Protection Board, *Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR* (European Data Protection Board, 8 October 2024) https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf accessed 30 July 2025, page 11.

⁸⁶ Qualtrics answer to SURF's question from the 11th August 2025.

According to Qualtrics' documentation, Education institutions act as controllers for the personal data processed by Qualtrics.

According to the privacy Policy, Qualtrics acts as the controller according to the following purposes:

- 1) To provide the services;
- 2) To communicate with the client about the services;
- 3) To improve, monitor, personalise, and protect the services;
- 4) For research and development;
- 5) For marketing and advertising;
- 6) For compliance and protection;
- 7) To train artificial intelligence tools.

These purposes are outside of the agreement with educational institutions and do not apply to Qualtrics' customers. According to Article 6 (4) GDPR, processing of personal data for a purpose other than the original one requires careful assessment (compatibility test). The controller must consider factors like the connection between the original and new purposes, the context of collection, the sensitivity of data, and potential impact on data subjects. If the vendor reuses the data (and customer data) on its own initiative, Qualtrics would be classified as the controller of this processing for the purposes mentioned in Privacy Policy.⁸⁷

A.8.3 Third Parties Involved in the Processing

Qualtrics maintains a list of subprocessors, categorizing them into mandatory and optional subprocessors. The mandatory subprocessors are based in the United States and India.⁸⁸ In the Table 12 Mandatory Subprocessors, the subprocessors list mentions the services of third parties that Qualtrics uses, and in which countries they are located.

Sub-processor	Based in	Purpose
Amazon Web Services	USA	Infrastructure / hosting services and storage, including backups. Software delivery and associated services.
Databricks, Inc.	USA	Infrastructure to streamline data ingestion, schematization assessment, and management.

⁸⁷ CNIL, 'Sous-traitants : la réutilisation de données confiées par un responsable de traitement' (8 June 2022) <https://www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement> accessed 30th January 2026.

⁸⁸ Qualtrics, 'Subprocessor List' (Qualtrics) <https://www.qualtrics.com/subprocessor-list/> accessed 30 July 2025.

Genesys	USA	Contact center support services.
IBM Cloud	USA	Data hosting facilities.
InfoCepts, LLC	India	Customer Service Centers for Support.
Wiz	USA	Cloud security management.

Table 12 Mandatory Subprocessors

A.9 Interests in Data Processing

This section outlines the (potential) interests of Qualtrics and the educational institutions. However, it does not address the fundamental data protection rights and interests of the data subjects. An analysis of how these rights interact with and relate to the interests of Qualtrics and the education organisations is provided in Part B of this DPIA.

A.9.1 Interests of Education organisations

Educational institutions have an interest in data-driven decision-making and fostering continuous institutional improvement. They use Qualtrics XM as part of their research and feedback ecosystems to achieve this. The platform enables the efficient distribution of large-scale surveys, facilitates usability testing, and supports the collection and analysis of both qualitative and quantitative data from students, staff, and other stakeholders.

They also have an interest in improving student engagement, academic satisfaction, and staff well-being, since these things are critical to institutional success. With actionable insights derived from experience data, universities and schools want to identify areas of improvement, respond proactively to concerns, and implement targeted initiatives to improve student retention, academic outcomes, and employee satisfaction.⁸⁹

Furthermore, they have an interest in carefully handling personal data, safeguarding privacy and complying with data protection laws.

A.9.2 Interests of Qualtrics

Qualtrics' interest in the Dutch education sector is driven by a mix of commercial opportunity, brand positioning, product development, and long-term institutional value. Serving this sector not only brings revenue but also enhances Qualtrics' credibility and competitive edge in the broader European public and academic markets. In order to determine the scope of the DPIA, SURF sent a survey to education institutions. The survey showed that the majority of education institutions use Qualtrics.

⁸⁹ Qualtrics, 'Student & Staff Experience Management for Education' (Qualtrics) <https://www.qualtrics.com/education/> accessed 30 July 2025.

A.9.3 Interests of data subjects

Data subjects such as students, faculty, and staff have several legitimate interests in the context of data collection and experience management conducted through Qualtrics XM.

The most foundational interest is that data subjects have a strong interest in the secure handling of personal data. They expect transparency and control of their personal data. Additionally, the feedback from data subjects contributes to improvements in curriculum design, student services, academic support structures. Additionally, some of the SURF members expressed the concern that this vendor occupying a monopolistic position on the market.⁹⁰

⁹⁰ SURF survey results from February 2025.

A.10 Processing Locations

The GDPR restricts transfers of personal data to countries outside the EEA unless adequate protection is ensured. This can be achieved through an adequacy decision by the European Commission or, in its absence, by using safeguards such as Standard Contractual Clauses (SCCs). Multinational organisations may also use Binding Corporate Rules (BCRs) for intra-group data transfers.

Qualtrics does not have BCRs. However, it relies on the SCCs between Qualtrics and education institutions (Customers), and between Qualtrics and its subprocessors. SCCs are legitimate to transfer personal data based on Qualtrics' self-assessment, and without obtaining the EDPB's approval decision as needed for the BCR to have a long-term compliance framework.⁹¹

In case of Qualtrics, the transfer is based on the SCCs and are governed by the EU SCC mentioned in Schedule 3 of the DPA.

The subprocessors and the transfers that take place are the following⁹²:

1. **Mandatory subprocessors:** USA and India.
2. **Mandatory Subprocessors Providing Content Delivery Network Services:** USA.
3. **Optional Subprocessors Offering Technical Functionality:** USA, Czech Republic, Ireland.
4. **Optional Subprocessors Offering Professional Services:** Canada, Hong Kong, Australia, Israel, USA, Italy, France, Australia, Brazil, Oman, Japan, Chile, South Korea, New Zealand, Germany, Taiwan, India, UK, Spain, Santiago de Chile, New Zealand, Colombia.

A.10.1 Adequacy decision

An adequacy decision means that the country in question has a level of protection comparable to that applied within the EEA. Currently, there are adequacy decisions with respect to Andorra, Argentina, Brazil, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay.

On 10 July 2023, the European Commission issued a renewed adequacy decision for the US. As a result, the US is considered to have an adequate level of data protection, and European organisations are allowed to transfer personal data to US based cloud service providers without any additional protective measures, provided that the importing organisations have registered themselves for these specific services, as a participant in the Data Privacy Framework.

As mentioned in Privacy Data Sheet, Qualtrics is self-certified under the EU-US Data Privacy Framework.⁹³

⁹¹ European Data Protection Board, 'Approved Binding Corporate Rules' (Our Work & Tools: Accountability Tools)https://www.edpb.europa.eu/our-work-tools/accountability-tools/bcr_en accessed 30 July 2025.

⁹² Qualtrics, 'Qualtrics Subprocessor List' <https://www.qualtrics.com/subprocessor-list/> accessed 30th January 2026.

⁹³ United States Department of Commerce, 'Data Privacy Framework List' (Data Privacy Framework, updated July 2025)<https://www.dataprivacyframework.gov/list> accessed 30 July 2025.

The new EU-U.S. data transfer agreement does not limit the authority of U.S. law enforcement agencies to compel disclosure of personal data belonging to Dutch customers under the U.S. CLOUD Act (Clarifying Lawful Overseas Use of Data). This legislation was specifically designed to enable access to data stored in data centers located outside the United States, including within the EU. The CLOUD Act extends the jurisdiction of U.S. courts to all data controlled by U.S.-based companies, regardless of where that data is physically stored.

As the European Parliament notes in its opinion on the Data Privacy Framework:

*"the EO [Executive Order from the President, added by Privacy Company] does not apply to data accessed by public authorities via other means, for example through the US Cloud Act or the US Patriot Act, by commercial data purchases, or by voluntary data sharing agreements."*⁹⁴

A.10.2 Standard Contractual Clauses

For educational institutions whose use of Qualtrics XM involves the transfer of personal data from the European Economic Area (EEA), the United Kingdom, or Switzerland to countries outside these jurisdictions, Qualtrics relies on established legal mechanisms to ensure adequate protection of personal data. Qualtrics primarily uses the Standard Contractual Clauses (SCCs) for the subprocessors where the DPA does not apply.⁹⁵

Standard Contractual Clauses (SCCs) are incorporated into its DPA and serve to safeguard data when it is transferred from Qualtrics LLC to the United States or other non-EEA affiliates. Qualtrics provides a self-service platform for customers to collect and process personal data, acting as a data processor while the customer serves as the data controller. Since Qualtrics Cloud Services involve international data transfers to countries without adequate protection, SCCs are used to ensure compliance and safeguard personal data.⁹⁶

If the Contractor is not in a third Country, it enters Module 3 of the SCCs with each Subprocessor and ensures that Subprocessors do the same when acting as data exporters. Similarly, if Qualtrics is not in a Third Country but subject to GDPR or other SCC requirements, it enters into SCCs with the Contractor for relevant data transfers.⁹⁷ Overall, Qualtrics relies on Module 2 (controller-to-processor) and Module 3 (processor-to-processor) of the New SCCs, since it only acts as a processor in its cloud services according to the DPA, and a controller for Qualtrics' own purposes.⁹⁸

⁹⁴ European Parliament, 'Adequacy of the Protection Afforded by the EU-US Data Privacy Framework' (European Parliament, 11 May 2023) https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html accessed 10 October 2025.

⁹⁵ Qualtrics, 'Standard Contractual Clauses Update' (Qualtrics, last updated c 3 years ago) <https://www.qualtrics.com/scc-update/> accessed 30 July 2025.

⁹⁶ Qualtrics, 'Standard Contractual Clauses Update' (Qualtrics, last updated c 3 years ago) <https://www.qualtrics.com/scc-update/> accessed 30 July 2025.

⁹⁷ Qualtrics, *Qualtrics Contractor Data Processing Agreement (CDPA)* (Qualtrics, last revised 15 March 2024) <https://www.qualtrics.com/cdpa/> accessed 30 July 2025.

⁹⁸ Qualtrics, 'Standard Contractual Clauses Update' (Qualtrics, last updated c 3 years ago) <https://www.qualtrics.com/scc-update/> accessed 30 July 2025.

SCCs are crucial for Qualtrics. Qualtrics office and support personnel maintains the platform in the EU but also outside the EU. The functions for the data processing outside of the EU include engineering, customer support, customer success for third party services (mandatory) in third countries such as USA and India.⁹⁹

According to the EDPB (European Data Protection Board) guidelines, *‘the SCCs and are sufficient to ensure that the level of protection guaranteed by the GDPR is not undermined. The data exporter and importer need to ensure that additional clauses cannot be construed in any way to restrict the rights and obligations in the SCCs or in any other way to lower the level of data protection.’*¹⁰⁰

Qualtrics SCCs describe the transfers including the description of the parties, transfers, and description of the competent supervisory authority, includes security measures, and subprocessors. This gives an opportunity for educational institutions to provide for a sufficient level of data protection and comply with the principle of accountability in theory.

Additionally, clauses for the ‘Transfers outside of the European Economic Area’ are mentioned in the Schedule 1 to the DPA. This is the place where an education institution gives the processor (Qualtrics) specific permission for the following transfers to third countries and includes additional security measures in place.

A.11 Legal and Policy Framework

The ePrivacy Directive significantly affects how organisations process personal data in the context of electronic communications. It complements the GDPR, providing more specific rules around privacy in the digital environment. This section elaborates in more detail. Additionally, this chapter will examine legally binding orders directed to Qualtrics and explore the internal procedures the company follows when responding to such requests.

A.11.1 ePrivacy Directive

Certain rules from the current ePrivacy Directive apply to the storage of information on, and retrieval of that stored information from, browsers with pixels and cookies and similar technologies such as tracking pixels. Consent is required prior to the retrieval or storage of information on the devices or browsers of end users, unless one of the exceptions applies, such as the necessity to deliver a requested service, or the necessity for the technical transmission of information.

The current ePrivacy Directive also includes rules on the confidentiality of data from the information provided by Customers, and on communication behaviour. Article 5(1) obliges Member States to guarantee the confidentiality of communications and related traffic data via public communications networks and publicly available electronic communications services.

⁹⁹ Qualtrics, ‘Qualtrics Subprocessors’ (Qualtrics, published c 5.2 years ago) <https://www.qualtrics.com/subprocessor-list/> accessed 30 July 2025.

¹⁰⁰ European Data Protection Board, ‘Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data’ (European Data Protection Board, 18 June 2021)

[https://www.edpb.europa.eu/system/files/2021-](https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasures_transfer_tools_en.pdf)

[06/edpb_recommendations_202001vo.2.0_supplementarymeasures_transfer_tools_en.pdf](https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasures_transfer_tools_en.pdf) accessed 10 October 2025, page 23.

Article 6(1) obliges providers of publicly available telecommunications services to erase or make the traffic data anonymous as soon as they are no longer needed for the purpose of the transmission of the communication.

Although the confidentiality rules in the ePrivacy Directive originally only covered classic telephony and internet providers, the scope was expanded significantly. Since the European Electronic Communications Code (EECC) became applicable law (21 December 2020)¹⁰¹, the confidentiality rules apply to all over-the-top communications services.

In case of Qualtrics, the cookies were collected even before the end-user pressed on ‘Consent button’ before logging in. Therefore, Qualtrics starts setting the cookies the moment a user lands on the homepage before the user has interacted with a cookie banner. This goes against Article 5(3) of the ePrivacy Directive.

A.11.2 Transparency report

The EU–US Data Privacy Framework supplements these rules by establishing safeguards to protect personal information transferred between the European Union and the United States. It aims to ensure that any data shared for the purposes of preventing, investigating, detecting, or prosecuting criminal offences is handled in a manner that respects fundamental privacy rights. A requesting country may use evidence or information from the requested country only for criminal investigations, urgent public security threats, or closely related non-criminal proceedings. Use for other purposes is allowed only if the data is public or the requested country gives prior consent.¹⁰² Additionally, Article 48 GDPR states that any judgment or decision from a third-country authority requiring a controller or processor to disclose personal data is not automatically enforceable in the EU.

Qualtrics does not publish transparency reports about government requests publicly. However, the clause 4.2 DPA Processing on Legal requirements states:

‘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.’

SURF asked Qualtrics to clarify this statement. The explanation we received from Qualtrics was the following:

‘Qualtrics will only comply with binding orders of governmental entities that have jurisdiction over Qualtrics or as otherwise required by law. Like many other technology companies, Qualtrics may occasionally receive a request from a law enforcement or other government agency seeking access to certain data, including access to data belonging to a customer.’¹⁰³

¹⁰¹ Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, L 321/36, 17 December 2018, URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN>

¹⁰² European Union, ‘Agreement with the United States on Mutual Legal Assistance’ (EUR-Lex) <https://eur-lex.europa.eu/EN/legal-content/summary/agreement-with-the-united-states-on-mutual-legal-assistance.html?fromSummary=28> accessed 30 July 2025.

¹⁰³ Qualtrics answers to SURF questions from the 10th June.

Furthermore, Qualtrics explains that it complies with binding orders from authorities, however, shares the statistics with their customers only with regard to:

Compliance with binding orders: Qualtrics' position is to only comply with binding orders of governmental entities that have jurisdiction over Qualtrics or as otherwise required by law. This applies to requests from law enforcement or other government agencies seeking access to certain data, including data belonging to a customer.

Notification to customer: Upon receiving such a request, Qualtrics will notify Customer of that legal requirement before processing. This notification is done in writing, and email is permitted. Qualtrics will provide reasonable written notice to allow the Customer to seek a protective order or other appropriate remedy. This notification will occur unless that law prohibits such notification on important grounds of public interest.

Limiting disclosure: Qualtrics will only disclose such information as is required by the governmental entity or otherwise required by law.

Confidential treatment: Qualtrics will use commercially reasonable efforts to obtain confidential treatment for any confidential information so disclosed.

SURF asked for more information from Qualtrics about the meaning of 'efforts to obtain confidential treatment'. In the response to SURF, Qualtrics explained that:

*'This is with regards to our compliance with binding orders of governmental entities that have jurisdiction of Qualtrics, this clause means that we use commercially reasonable efforts to obtain confidential treatment for any confidential information disclosed pursuant to the Request.'*¹⁰⁴

Under the GDPR, any transfer of EU personal data to non-EU countries must ensure an 'essentially equivalent' level of protection. The CLOUD Act allows the United States (U.S.) authorities to compel access to data held by the U.S. companies, even if that data is stored in the EU. 'Qualtrics does not purposefully create back doors or other undocumented functionalities with the intention of unauthorized access to the system and/or data. Qualtrics will inform the Customer of any legally binding request from a public authority to access Customer data, to the extent Qualtrics is permitted to do so.'¹⁰⁵

Such non-disclosure may also conflict with the principle of transparency, which requires that personal data be processed in a manner that is clear, open, and accessible to data subjects (Article 5(1)(a) GDPR). Upholding this principle is essential to ensure individuals are informed about how their data is used, reinforcing both trust and legal compliance.¹⁰⁶

¹⁰⁴ Qualtrics answers to SURF questions from the 11th of August 2025.

¹⁰⁵ Qualtrics answer to SURF questions from the 10th of June.

¹⁰⁶ Recital 39 – GDPR. *It emphasizes that individuals should be aware of the collection and use of their personal data, including the extent and purpose of processing. This supports the idea that secrecy or non-disclosure can undermine transparency.*

A.12 Retention Periods

A controller may retain personal data as long as it is necessary for the purpose for which it was collected, the GDPR states (Article 5(1)(e) GDPR). After that, the controller must destroy the data, unless the controller is obliged to keep it longer, for example because it is provided for in a law. The latter should be set out in the processor agreement or otherwise similar agreement. This section describes the retention periods Qualtrics applies in its role as data processor and data controller.

Qualtrics supports data retention periods through retention policies, which define how long survey responses or contact data are stored.¹⁰⁷ These policies run every 24 hours, automatically deleting data older than the set limit.¹⁰⁸ Exceptions can be made for specific surveys with different retention needs. Additionally, anonymisation policies can be configured to remove identifying information from responses after a defined period, ensuring compliance with data protection requirements.

*'Qualtrics creates data backups, and these data backups are retained for up to 90 days. Restoration from these backup datasets is for disaster recovery only. Qualtrics' standard data deletion policy dictates the timeline for removing data, including from backups. When a user deletes data from the active database (or, if not deleted by the user, once the subscription term expires), that data will be fully removed from the active platform within 90 days. Following this, the data will be removed from all backups within an additional 90 days. This process means that data deleted by a user, or data remaining after subscription termination, will be completely deleted from Qualtrics systems within approximately six months.'*¹⁰⁹

The information provided by Qualtrics is demonstrated in the table Table 13 Data backups below.

Stage	Action	Retention Period	Purpose / Notes
Data Backup Creation	Regular backups of data	Up to 90 days after creation	Used only for disaster recovery
User-Initiated Deletion	Data deleted from active database	Removed within 90 days after deletion	When user removes manually and the subscription term expires
Subscription Termination	Expiry of user account triggers deletion	Within approximately 6 months	Same timeline as manual deletion

¹⁰⁷ Qualtrics, 'Data Retention' (Qualtrics Support) <https://www.qualtrics.com/support/survey-platform/sp-administration/data-privacy-tab/data-retention/> accessed 30 July 2025.

¹⁰⁸ Qualtrics, 'Data Retention' (no date) <https://www.qualtrics.com/support/survey-platform/sp-administration/data-privacy-tab/data-retention/> accessed 17 March 2026.

¹⁰⁹ Qualtrics answers to SURF legal questions (10th June 2025).

Backup Deletion	Deletion from backup systems	Additional 90 days to the original retention period of 90 days.	Ensures recovery risk is minimised
Final data erasure	Full removal from active and backup systems	Approximately 6 months total (90 + 90 days)	Completes deletion lifecycle

Table 13 Data backups

For the backup data retention, Qualtrics specifies that the litigation hold, a formal instruction to ‘freeze’ certain information so it is not deleted or changed, is under Customer’s control.

‘Regarding a request for a litigation hold, because the Brand is under the Customer’s control, it is up to the Customer to implement a litigation hold. Qualtrics has the ability to disable the entire Brand, meaning the Customer will have no access. Even so, Qualtrics cannot typically legally represent anything related to a Brand’s usage or Data for litigation purposes.’¹¹⁰

Retention periods of the personal data processed on behalf of the Controller (education institutions) are mentioned in Schedule 1 DPA. This is based on the choice of the institutions which retention period is used for any category of personal data together with the criteria to determine the period.

SURF requested more information about the processes that allow Qualtrics handle different retention periods assigned by educational institutions. Qualtrics’ response is the following:

‘We process based off of customer instruction/activity within their brand(s). E.g. Customer A may have an automated retention period set for all of their data, customer B may manually delete their data and customer C may not delete their data at all until the agreement ceases. These preferences will be adhered to before our Backup Management program is in place and data is ultimately erased out of services.’¹¹¹

¹¹⁰ Section ‘Backup Data Retention’ in Qualtrics’ Cloud Security & Privacy Framework from April 2025.

¹¹¹ Qualtrics’ answers to SURF from December 2025.

Part B Assessment of Lawfulness of Data Processing

The second part of the DPIA assesses the lawfulness of the data processing. This part contains an assessment of the legal grounds of both the educational institutions and Qualtrics, the processing of special personal data, the application of purpose limitation, the necessity of the processing and the application of data subject's rights.

B.1 Legal Basis

To comply with the GDPR, the processing of personal data must be based on one of the legal bases outlined in Article 6(1) of the Regulation.

Before addressing the applicable legal bases for the processing, it is first necessary to outline the context in which the processing occurs. This includes not only defining the roles of the parties involved but also examining the contractual framework that governs their relationship.

B.1.1 Contractual context and role determination

B.1.1.1 DPA concluded via [REDACTED]

Education institutions conclude two types of the DPAs through SURF DPA model: directly with Qualtrics and through the provider [REDACTED] which distributes the Qualtrics products to educational institutions in the Netherlands.¹¹² The scope of the later agreement is 'DAS uitvraag Online Collaboration tools, perceel 3 Polling&Survey tools'.¹¹³

The role determination is undermined due to the fact that there is no defined relationship between the educational institution as controller and Qualtrics as processor according to the DPA. In this agreement, there is a direct agreement between the controller and [REDACTED], and not Qualtrics which does not correspond to the requirements of Article 28 GDPR.

*'Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.'*¹¹⁴

EDPB states that the the processing agreement should be specific and directly address the controller-processor relationship.¹¹⁵ The processor is [REDACTED] according to the agreement, together with Qualtrics. [REDACTED] is the only contractual party who signs the agreement. This does not create a direct binding agreement with Qualtrics, or that the reseller's agreement effectively binds Qualtrics to the controller's instructions. In the agreement, there is the

¹¹² [REDACTED]

¹¹³ Annex 4 Data Processing Agreement 'Online Collaboration tools' (based on SURF Model Data processing Agreement version 3.0 from January 2019), date 24th October 2023, page 2.

¹¹⁴ Article 28 GDPR.

¹¹⁵ EDPB, https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf, page 4.

reference only to the ‘DAS uitvraag Online collaboration tool, perceel 3 Polling & survey tools’. There is no reference to the names of the services that Qualtrics offers to the institution, but a general name of the services offered that the seller distributes to the education institutions.

The issue of the service names was also experienced by SURF when the scope of the research had to be determined. Since this information could not be clearly derived from the agreement, SURF looked for the clarification directly from Qualtrics, and Qualtrics provided the necessary details of the services that educational institutions use. As identified by the EDPB: *‘Therefore, the processing agreement should not merely restate the provisions of the GDPR: rather, it should include more specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement.’*¹¹⁶ Therefore, if the agreement lacks the concrete and specific information, it should be provided to fulfill the principle of accuracy of the data processing.

Additionally, since the allocation of the responsibilities is not defined clearly and not linked directly to Qualtrics, the protection of rights and freedoms of data subjects as well as responsibility are jeopardized due to non-clear allocation of responsibility and liability of controller and processors.¹¹⁷ Specifically, that Qualtrics was not mentioned in this agreement, although Qualtrics’ services are used. Therefore, for education institutions, it is important to draft a DPA with clear indications of the parties’ roles to the DPA agreement.

B.1.1.2 Misalignment with the role allocation in Schedule 1 of the DPA, Privacy Policy and GTC

According to the statements available publicly and Qualtrics’ responses to SURF, Qualtrics operates as a data agnostic platform. *‘All Customer Data is considered highly confidential, treated equally, and protected using industry-best practices, regardless of whether it is sensitive or not.’*¹¹⁸ However, following the technical research, SURF identified that there are cases of misalignment of the purposes of data processing activities with the role of Qualtrics.

In Privacy Policy, which is applicable only to Qualtrics’ website visitors and not Customers, it is mentioned that Qualtrics may process personal data for the purpose of Service development such as release, development, and upload of any fixes or upgrades to the Cloud services.

The similar purpose is observed in Schedule 1 to the DPA where the vendor may process the transferred personal data for the ‘Release, development, and upload of any fixes or upgrades to the Cloud Service’.¹¹⁹

¹¹⁶ European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (July 2020) https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf accessed 10 October 2025. page 32.

¹¹⁷ European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (July 2020) https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf accessed 10 October 2025. page 32.

¹¹⁸ Qualtrics’ responses to SURF questions from the 9th of December.

¹¹⁹ [https://success.qualtrics.com/rs/542-FMF-](https://success.qualtrics.com/rs/542-FMF-412/images/Qualtrics%20GTC%20DPA%20%28for%20Online%29%20Template%20250523-MJR.pdf?version=0)

[412/images/Qualtrics%20GTC%20DPA%20%28for%20Online%29%20Template%20250523-MJR.pdf?version=0](https://success.qualtrics.com/rs/542-FMF-412/images/Qualtrics%20GTC%20DPA%20%28for%20Online%29%20Template%20250523-MJR.pdf?version=0)

In the GTC, there is a clause that *‘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.’*¹²⁰ This clause describes a processing activity. Placing this clause in the GTC rather than the DPA creates a misalignment with the The processing activity requires a legal basis such as the DPA framework. If the anonymisation happens before the analysis, the process of anonymizing is itself personal data processing. This process is governed nowhere in the DPA.

Qualtrics explains that:

‘Qualtrics does not use raw Customer Data to train its own models. It uses anonymized and aggregated Customer Data for any model training purposes. Furthermore, Qualtrics has contractual agreements and specific configurations with third-party Large Language Model (LLM) providers (subprocessors) to ensure that Customer data shared with them will not be utilized for AI/LLM training purposes by the vendor or retained by them.

*for the purpose of "Service Development," Qualtrics only uses a subset of Customer Data (Anonymized and Aggregated Analyses) that no longer constitutes Personal Data, effectively preventing any "intersection" with its controller purpose of "research and development" which uses its own collected data.’*¹²¹

Regarding the DPA, no clauses about restriction of further LLM training on anonymised personal data are mentioned. The DPA with education institutions, Article 2.3.3, prohibits the processing for the benefit of the vendor or third-parties, or for advertising, or other purposes. No agreements were observed with education institutions about the LLM training.

For the anonymisation, as was discussed in Section A.6.4, only few personal data categories are flagged and anonymised. The anonymisation technique excludes entirely special types of personal data.

Therefore, by processing personal data for its own purpose such as ‘Service development’, Qualtrics is processing beyond the instructions of the education institutions. Even if Qualtrics uses anonymisation techniques, the legal threshold for anonymisation is high. If the anonymisation technique fails or does not detect special categories of personal data to prevent re-identification, Qualtrics is processing personal data for its own strategic ends. Recital 26 of the GDPR provides that all means of reidentification that could reasonably be used must be taken into account, such as the nature and volume of data. Anonymisation is a processing activity in itself because according to Article 4 (2) GDPR:

‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

¹²⁰ Qualtrics, *‘Qualtrics GTC DPA (for Online) Template’* (no date), Clause 3.4, <https://success.qualtrics.com/rs/542-FMF-412/images/Qualtrics%20GTC%20DPA%20%28for%20Online%29%20Template%20250523-MJR.pdf> accessed 17 March 2026.

¹²¹ Qualtrics’s responses to the SURF questions on the 9th December 2025.

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'

Therefore, Qualtrics should mention this in the Data Processing Agreement which is concluded with education institutions.

B.1.1.3 Governing Law and Disputes

Additionally, according to the Clause 12.10 'Governing Law and Disputes', *'Agreement and any claims: 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.'*

Even though, the GDPR strong enforcement applies regardless of the GTC terms, from the consumer law protection, it is not clear for the customer which terms and laws apply in case of a dispute. This might create jurisdictional disadvantage for the education institutions. Whereas consumers, in cross border disputes, can bring action in their own Member State of domicile or the seller's.¹²²

The interplay between the GTC and mandatory EU law leaves customers in a state of legal uncertainty. The consumer law protection are weakened when the vendor defaults to Delaware law, where the transparency obligations are not the same as expected by education institutions. This creates a jurisdictional disadvantage for the education institutions.

The GTC has reference to the Qualtrics Responsibilities such as 'Providing support for the Cloud Services as referenced in the order form'.¹²³ It was mentioned in Section A.1.6 Educational institutions' order forms, that order forms mention special categories of personal data. This creates a risk to the transparency for the data subject; while the processing may occur across various regions, the governing jurisdiction established by the GTC is Delaware rather the Member State. This is due to the Order Form being referenced by the GTC which is governed by Delaware law.

B.1.2 Legal grounds

Article 6, paragraph 1(e) of the GDPR (Task carried out in the public interest).

Institutions have a legal obligation to perform a public task, namely the organisation of education.

In order to perform this task, institutions must draw up plans and schedules, and the processing of personal data is necessary to do so. To invoke this basis, institutions must carry out a necessity test to demonstrate that the processing is necessary for the proper performance of

¹²² The Brussels I Regulation (Recast) Regulation 1215/2012, articles 17-19.

¹²³ Qualtrics General Terms and Conditions, Clause 3.2.

their public task. For the processing of data that is not necessary for their public task, institutions may be able to apply one of the following bases.¹²⁴

Article 6, paragraph 1(a) of the GDPR (Consent)

To process users' personal data such as particular consent part of the surveys to process sensitive data, special categories of data, or even IP address, the consent should be requested from the user (data subject) via the platform.

Among other things, this consent must be freely given to be valid as a basis under the GDPR. This means that the user must not suffer any adverse consequences from refusing consent. Institutions must therefore provide users with sufficient information about the interactions in Qualtrics if they wish to explicitly consent to the services.

Article 6(1)(b) of the GDPR (Performance of a contract)

Processing that is not necessary for the performance of a public task may be necessary to perform a contract with students (e.g. an education contract) and/or employees (e.g. an employment contract). Here too, institutions must carry out a necessity test to demonstrate that the purpose of the contract cannot be achieved without the processing of personal data in question.¹²⁵

Qualtrics states that Customers are responsible for ensuring compliance specifically, accuracy and transparency.¹²⁶ However, the burden of compliance is shifted mainly to education institutions despite the DPA in place according to which the vendor should assist the Controllers with data processing activities. From the vendor's side, there is no transparent and accessible data-to-purpose mapping, for instance, Records of Processing Activities ('ROPA') of Customers personal data. Without insight into which specific data categories are being used for concrete processing activities, the Customer may not fulfill its duty to inform data subjects or ensure data integrity.

These aspects are absent from the definitions provided in the GTC. Specifically, under Article 28 GDPR as discussed by the EDPB:

*'When a processor processes data outside or beyond the controller's instructions, and this amounts to a decision determining the purposes and means of processing, the processor will be in breach of its obligations and will even be considered a controller in respect of that processing in accordance with Article 28(10).'*¹²⁷

While the privacy policy draws a distinction between Customer data and 'other information' such as service usage data, account data, and marketing data, there is no information about the categories/list of personal data that Qualtrics processes on behalf of education institutions or as an independent controller. For instance, account creation details, school setup information,

¹²⁴ Wet open overheid, Wet open overheid (Stb. 2021, 358) <https://wetten.overheid.nl/BWBR0005682/2025-01-01> accessed 10 October 2025.

¹²⁵ Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) of the GDPR in the context of the provision of online services to data subjects, EDPB

¹²⁶ Qualtrics' feedback from the 21st February 2026.

¹²⁷ https://www.edpb.europa.eu/system/files/en?file=2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf, page 36.

contact data and certain log data (like IP addresses) appear in both. Common identifiers such as name and email address are mentioned in both the DPA and the 'other information' section of the privacy policy. This overlap between personal data and purposes of the processing blurs the line between the data processed on behalf of the institution and data processed for Qualtrics' own purposes, making it difficult to clearly define the roles and responsibilities.

Article 6(1)(f) of the GDPR (Legitimate interest)

Processing that is not necessary for the performance of a task carried out in the public interest may be necessary for the purposes of the legitimate interests pursued by the institution. In order to use this basis, it must be assessed whether institutions (1) have a legitimate interest, (2) the processing is necessary to pursue this interest, and (3) whether the interests of the institution outweigh those of the data subjects.¹²⁸

B.1.2.1 Legal grounds for Qualtrics

B.1.2.1.1 Consent

Consent can make processing of personal data lawful, if and to the extent that the purposes are specific (Article 6 (1) (a) GDPR). When processing has multiple purposes, consent should be asked for all of them separately. Article 4 (11) GDPR, defines 'consent' as meaning 'any freely given, specific, informed and unambiguous indication of the data subject's wishes which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

The fact that education and research institutions are public sector organisations also makes it difficult to rely on consent for processing. In the context of Recital 43 of the GDPR, the EDPB explains: *"whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. The EDPB considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities."*¹²⁹

Meanwhile, when Qualtrics acts as a processor, there is no obligation on Qualtrics to obtain the consent from customers. It is a direct responsibility of Controllers which stems from the agreement. However, Qualtrics may enhance its privacy by design choices to help its customers in obtaining valid consent from its data subjects.

For example, as was discussed in Section A.4.6.1, it was observed that the consent banner does not include an option to 'Reject all cookies'. This will correspond to the practice of informed consent, where a user has a genuine freedom of choice to reject or accept the cookies: 'Rejecting must be as easy as accepting'.¹³⁰

Whereas, Qualtrics elaborated the consent functionality as: *'The process involves the Customer's end users accessing Qualtrics' products via modern web browsers, with all access to the front-end*

¹²⁸ Autoriteit Persoonsgegevens, 'Basis AVG: Grondslagen AVG Uitgelegd – Gerechvaardigd Belang'

<https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslagen-avg-uitgelegd#grondslag-gerechvaardigd-belang> accessed 10 October 2025.

¹²⁹ EDPB, Guidelines on consent, paragraph 3.1.1.

¹³⁰ [Judgment of the Hanover Administrative Court dated 19.03.2025 \(10 A 5385/22\)](#)

*Cloud Service using HTTPS (Hypertext Transfer Protocol Secure) and enforcing HSTS (HTTP Strict Transport Security).*¹³¹

B.1.2.1.2 Necessity for the performance of the contract

The legal ground of necessity for the performance of a contract (Article 6(1)(b) GDPR) is limited to situations where the processing is strictly necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

This legal ground can be used in this situation. Because Qualtrics and educational institutions conclude a GTC and DPA. The DPA (the Qualtrics' template) outlines the responsibilities, and even though there is a DPA in place, a more detailed and specific DPA should always be in place between educational institutions and Qualtrics for detailed compliance, especially when processing is done on behalf of a controller by a processor.¹³²

Since the GTC references and governs the Order Form, the data subjects special categories of data are governed by this agreement. Despite the absence of a direct agreement between the data subject and Qualtrics, the vendor's contractual practice indirectly affects the individual's data protection interests. Potentially, the special categories might fall outside of the DPA framework.

B.1.2.1.3 Necessity to comply with a legal obligation

Article 6 (1) (c) GDPR reads: *"processing is necessary for compliance with a legal obligation to which the controller is subject"*. There are four conditions that need to be met for this legal basis to be relied on:¹³³

- the legal obligation must be defined by EU or national law to which the controller is subject;
- these legal provisions must establish a clear and specific obligation to process that personal data;
- these provisions must at least define the purposes of the processing;
- this obligation should be imposed on the controller and not on the data subject.

If these criteria are not fulfilled, the processing operation cannot rely on the legal ground 'to comply with a legal obligation'.

According to the DPA, there is an obligation for the Processor to only cooperate with the request or order if the processor is legally obliged to do so and, where possible, the processor shall (judicially) object to the request or order or the prohibition to inform the controller about this or

¹³¹ Qualtrics' responses to SURF questions from the 9th December.

¹³² European Data Protection Board, 'Process Personal Data Lawfully' (EDPB SME Data Protection Guide) https://edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_en#toc-4 accessed 10 October 2025.

¹³³ European Data Protection Board, 'Process Personal Data Lawfully' (EDPB SME Data Protection Guide) https://edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_en#toc-4 accessed 10 October 2025.

to follow the instructions of the controller.¹³⁴ Therefore, the lawful ground ‘necessary to comply with a legal obligation’ might be applicable for the data processing.

Therefore, for further processes due to the judicial request or orders, Qualtrics may become a controller with the legal ground of ‘*complying with a legal obligation to which the controller is subject*’. Qualtrics elaborated that this assessment will be entirely fact dependent.¹³⁵

B.1.2.2 Legal grounds for educational institutions

B.1.2.2.1 Consent

Educational institutions should refrain from asking for consent from students and employees for the processing of their personal data. In view of the imbalance of power between students and educational institutions, consent can seldom be given freely.¹³⁶ Employees and students may not be free to refuse or withdraw consent for the processing of their personal data without facing adverse consequences.

According to the GTC, Qualtrics puts the main responsibility on the customer to obtain consent from data subjects:

‘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.’¹³⁷

In order to base the processing on the lawful ground, education institution requests the consent for the processing from the data subject. Based on the technical and legal analysis conducted by SURF, there is more personal data being processed by Qualtrics than the data subject consented to such as location data. Qualtrics believes that this is up to the institution to provide the data subject with the relevant processing activities.¹³⁸

¹³⁴ SURF model DPA “DAS uitdraag online collaboration tools, perceel 3 Polling & survey tools”. Section 3.3.2.2.

¹³⁵ Qualtrics’ feedback from the 21st of February 2026.

¹³⁶ Recital 49 GDPR: The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security.

¹³⁷ Qualtrics, ‘Qualtrics GTC & DPA Template’ (Qualtrics Success, 25 May 2023) <https://success.qualtrics.com/rs/542-FMF-412/images/Qualtrics%20GTC%20DPA%20%28for%20Online%29%20Template%20250523-MJR.pdf?version=0> accessed 10 October 2025, section 2.2 of the GTC.

¹³⁸ Qualtrics’ feedback from the 21st of February 2026.

B.1.2.2.2 Necessity for the performance of a contract

The legal ground of necessity for the performance of a contract (Article 6 (1) (b) GDPR) is limited to situations where organisations have contract with specific data subjects (such as an employment contract or an education agreement), and the processing is strictly necessary to perform the contract with such individual data subjects. The European Data Protection Authorities explain: *“The controller should be able to demonstrate how the main object of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur. Thus, this ground can never be invoked by a party that does not have its own contract with that individual.”*¹³⁹

If controllers want to rely on the ground of performance of a contract, the processing must pass the necessity and proportionality tests. In particular, the controller must assess whether the purpose for which the personal data are processed cannot reasonably be achieved in another way which is less prejudicial to the persons involved in the processing of personal data.¹⁴⁰ The CJEU has a strict interpretation of the ‘necessity’ requirement. In order for the processing of personal data to be regarded as necessary for the performance of a contract, within the meaning of that provision, the processing must be *“objectively indispensable for a purpose that is integral to the contractual obligation intended for the data subject.”*¹⁴¹ The controller must therefore be able to demonstrate how the main subject matter of the contract cannot be achieved if the processing in question does not occur.¹⁴² In the case of *Meta vs Bundeskartellamt* the CJEU considers: *“The fact that such processing may be referred to in the contract or may be merely useful for the performance of the contract is, in itself, irrelevant in that regard. The decisive factor ... is rather that the processing of personal data by the controller must be essential for the proper performance of the contract concluded between the controller and the data subject and, therefore, that there are no workable, less intrusive alternatives.”*¹⁴³

The legal ground of contract cannot be invoked by organisations for the processing of personal data of data subjects that do not have a contractual relationship with that organisation. Furthermore, the educational institutions cannot invoke the legal ground of contract for the processing of personal data for purposes that are not necessary for the performance of the contract with each individual data subject.

If the processing is not necessary to deliver what the contract promises, then an educational institution cannot rely on the contract to justify that processing. It must find a different legal basis such as consent or legitimate interest.

Transparency is key: individuals must be informed about the use of Qualtrics, the purpose of data collection, and their rights.

¹³⁹ EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, paragraph 26 and 30.

¹⁴⁰ ABRvS 20 September 2017, ECLI:NL:RVS:2017:2555.

¹⁴¹ CJEU 4 July 2023, ECLI: EU:C:2023:537 (*Meta vs Bundeskartellamt*) paragraph 98.

¹⁴² EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation, 16 October 2019, nr. 13. URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.

¹⁴³ CJEU 4 July 2023, ECLI: EU:C:2023:537 (*Meta vs Bundeskartellamt*) paragraph 99.

B.1.2.2.3 Processing is necessary for a task in a public interest or for the legitimate interests of the controller or a third party

Article 6 (1) (e) GDPR reads: *“processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”*.

It follows from the CJEU ruling *Meta vs Bundeskartellamt* that a task of public interest within the meaning of Article 6(1)(e) GDPR is not sufficient as a basis for data processing in itself. Lawful processing of personal data on the basis of Article 6(1)(e) GDPR presupposes not only that a task of public interest is thereby performed, but also that the processing is based on EU law or on Member State law to which the controller is subject, and that that legal basis must meet an objective of public interest and be proportionate to the legitimate aim pursued (Article 6 (3) GDPR).

B.2 Special Categories of Data and Sensitive Data

Qualtrics mentioned in the responses to SURF, that it processes the customer data on behalf of the customers. The list of personal data was not provided to SURF, and SURF could not map the processing of personal data to separate processing activities based on the information stemming from Schedule 1 DPA. It also was not possible to establish which special categories of personal data Qualtrics processes. The education institution determines which types of special categories of personal data are processed, and Qualtrics does not classify the data regardless the data is owned by the institutions.¹⁴⁴

However, sensitive data is discussed in Qualtrics' documentation. Regarding the Sensitive Data Policy, Qualtrics explained that Customer should configure the policy to redact certain specific informatin, and customers can choose to create their own Sensitive Data Policy to identify BSN, for example.¹⁴⁵ In the Section A.6.5, SURF discussed that for highly sensitive data, like credit card numbers or Social Security Numbers (bsn), this data may be automatically redacted when it is collected. This means that it is hidden and irretrievable for both Qualtrics and education institutions.

BSN and credit card do not fall within the categories of personal data mentioned in Article 9 GDPR such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships. However, bsn is linked to financial information such as account balances or assets, with the government. This classifies bsn as sensitive information. According to the Dutch Data Protection Authority, it is only possible to use the bsn if the law states that an organisation is allowed to do so.¹⁴⁶

*'For the government, the use of the BSN is regulated in Article 10 of the General Provisions Civil Service Number Act (Wabb). It states that government organizations may use the BSN if necessary to carry out their public task.'*¹⁴⁷

Therefore, the processing of BSN falls within the processing of the categories of sensitive personal data.

¹⁴⁴ Qualtrics' repsonse from the 21st February 2026.

¹⁴⁵ Qualtrics' response from the 27th March, 2026.

¹⁴⁶ Autoriteit Persoonsgegevens, 'Voorwaarden gebruik BSN'

<https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/burgerservicenummer-bsn/voorwaarden-gebruik-bsn> accessed 10 October 2025.

¹⁴⁷ Ibid.

B.3 Purpose Limitation

The requirement that the provision of information to, and communication with, data subjects is done in a “concise and transparent” manner means that data controllers should present the information/communication efficiently and succinctly in order to avoid information fatigue.¹⁴⁸

The principle of purpose limitation is that data may only be “*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) GDPR not be considered to be incompatible with the initial purposes*” (Article 5(1)(b) GDPR). In essence, this means that a controller must specify a clear and specific purpose for collecting personal data and ensure that any further processing remains compatible with that original purpose.

In its privacy policy, Qualtrics mentioned that: *‘We may process personal information using artificial intelligence (AI) technologies including generative AI, and we use this information for training machine learning models, natural language processing, large-language models and other relevant AI use-cases.’*¹⁴⁹

Indeed, during the technical research, we mentioned that Qualtrics processes personal data for its own purposes such as training of its AI and machine learning models. See Section on Internal Purposes. The anonymised or aggregated data is used for these purposes. Since the internal processes within Qualtrics are not transparent, SURF could only deduce the methods of anonymisation that Qualtrics implements.

Qualtrics offers several privacy-oriented features such as anonymity thresholds, pseudonymisation options, anonymous survey settings, and automated anonymisation policies. Many of the protections are optional, not enabled by default, or limited in scope (pseudonymisation vs. full anonymisation). Most critically, the platform’s method for detecting and removing customary personal data relies on proprietary algorithms whose workings and effectiveness remain unclear to users. As such, Qualtrics is not transparent in how it implements and enforces privacy and anonymisation measures.

In order to determine if the purposes are compatible with the subsequent purpose, there should be a possible link between the purposes for which the personal data were collected and the purposes of the further processing envisaged.¹⁵⁰ However, SURF reviewed the agreements and observed that education institutions did not include the purpose to train AI models based on the anonymised data without confirming the technology used for the anonymisation and did not agree for the anonymisation of the personal data to train LLM in the agreements. These purposes are not compatible with the purposes that education institutions instructed Qualtrics with according to the DPA.

¹⁴⁸ European Data Protection Board, Guidelines on Transparency under Regulation 2016/679 (WP260rev01, 11 April 2018) https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf accessed 10 October 2025, page 7.

¹⁴⁹ Qualtrics, “Privacy Statement” <https://www.qualtrics.com/privacy-statement/> accessed 10 October 2025.

¹⁵⁰ CNIL, ‘Sous-traitants : la réutilisation de données confiées par un responsable de traitement’ (8 June 2022) <https://www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement> accessed 30th January 2026.

B.4 Necessity and Proportionality

The concept of necessity is made up of two related concepts, namely proportionality and subsidiarity. The personal data which are processed must be necessary for the purpose pursued by the processing activity. Proportionality means the invasion of privacy and the protection of the personal data of the data subjects is proportionate to the purposes of the processing. Subsidiarity means that the purposes of the processing cannot reasonably be achieved with other, less invasive means. If so, these alternatives have to be used.

Proportionality demands a balancing act between the interests of the data subject and the data controller. Proportionate data processing means that the amount of data processed is not excessive in relation to the purpose of the processing. If the purpose can be achieved by processing fewer personal data, then the controller needs to decrease the amount of personal data to what is necessary according to Article 5.

B.4.1 Assessment of proportionality

The key questions are: are the interests properly balanced? And does the processing not go further than what is necessary?

To assess whether the processing is proportionate to the interest pursued by the data controller(s), the processing must first meet the principles of Article 5 of the GDPR. As legal conditions they have to be complied with in order to make the data protection legitimate.

Lawfulness

The public documentations such as publicly available GTC, privacy policy, and private documentations like SURF model data processing agreement, and Trust Centre were reviewed by SURF to assess the lawfulness and legal grounds of the processing.

Overall, Qualtrics relies on the ground of 'necessary for the performance of the agreement'. Qualtrics bases their processing on the DPA between educational institutions and Qualtrics. However, due to the lack of the direct link concluded in a DPA between educational institution, reseller and Qualtrics, the legal ground may be not only directly applicable to a vendor.

The lawfulness of the processing is based on the consent that data subjects provide for the processing of their personal data. For instance, a student completing a research survey thorough Qualtrics services has no direct contractual relationship with Qualtrics. Article 6 (1) (b) cannot be invoked neither by an education institution nor the vendor for processing student data.

Fairness

Fairness is an overarching principle which requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected, or misleading to the data subject.¹⁵¹ There are several circumstances that might be unexpected for the data subject. If processing causes negative effects, those must be justified and proportionate.

According to Qualtrics, educational institutions, as data controllers, are responsible for determining the purposes and means of data processing. However, personal data might be used in an unexpected way. SURF cannot verify the models. It is important to highlight that Qualtrics' lack of technical transparency makes it impossible to fully assess the fairness, explainability, or reliability of the AI or ML methods used. Specifically, the usage of the anonymised personal data for further data processing activities such as training LLM undermines the transparency and purpose limitation principles.

Transparency

The principle of transparency not only ensures that consent must be informed but that full transparency of data practices and rights is ensured to users. In the case of children, this means that information relating to data processing must be comprehensible, recognisable and accessible to them (Article 12 GDPR).

Principle of transparency might be undermined with the usage of generic purpose descriptions and uses words as 'like' or 'for example'. In general, the use of ambiguous wording or vague terms can contradict the principle of fairness of Article 5 (1, a) GDPR, since information cannot be considered transparent, making data subjects unable to understand the processing of their personal data and to exercise their rights. According to the EDPB, the use of conditional tense ("might") leaves users unsure whether their data will be used for the processing or not." The EDPB recalls that the use of conditional tense or vague wording does not constitute "clear and plain language" as required by Article 12 (1) phrase 1 GDPR and may only be used if controllers are able to demonstrate that this does not undermine the fairness of processing.

The information that was provided in the section DSAR Service Outcomes, shows that Qualtrics is not transparent regarding the extensive data processing activities where Qualtrics acts as a data controller and as a data processor. Specifically, the information was missing from the following data processing activities such as:

1. Website and service usage analytics data. This relates specifically to unique identifiers that might be linked to the user's activity for the purpose of service improvement. SURF's technical investigation showed that third-party analytics services were used from Amplitude, Pendo, and Google Analytics.
2. Marketing, Advertising, and Profiling Data to build user profile.
3. Support, community and training data: generating personal data for which Qualtrics is a controller for the services Qualtrics Support, XM Basecamp, and Qualtrics Community.

¹⁵¹ EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and Default, version 2.0, adopted on 20 October 2020, p. 16, URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

4. General account metadata and browser information such as collecting and analysing information of visitors, including the domain name, visited surveys, referring Uniform Resource Locators (URLs) and other publicly available information.¹⁵²

SURF does not have documentation from Qualtrics specifying which data processing and which purposes are explicitly covered under the agreed terms between Qualtrics and the educational institutions for the role of processor. Without this documentation, SURF is relying solely on Qualtrics' public statements and Trust Center information. However, these sources do not provide a complete overview of the data flows, categories of personal data processed, purposes, methods, or other essential details required for full transparency from the vendor.

Therefore, Qualtrics does not demonstrate adherence to the transparency principles relating to processing of personal data towards the educational institutions according to Article 5 (1,a) GDPR, thereby not enabling the educational institutions as controllers to be transparent to their data subjects.

Data minimisation and privacy by design

The principles of data minimisation and privacy by design require that the processing of personal data be limited to what is necessary. The data must be '*adequate, relevant and limited to what is necessary for the purposes for which they are processed*' (Article 5(1)(c) of the GDPR). This means that the controller may not collect and store data that are not directly related to a legitimate purpose. According to this principle, the default settings for the data collection should be set in such a way as to minimise data collection by using the most privacy friendly settings.

The principle of "data minimisation" precludes the combination, analysis and processing of all personal data obtained from the data subject or third parties by a controller, such as the operator of an online social media platform, and collected both on that platform and elsewhere, for the purposes of targeted advertising, without any limitation in time and without distinction as to the nature of that data.¹⁵³

SURF submitted the DSAR requests to have a more clear picture on the purpose of the processing and the categories of personal data. The DSAR response were not complete. It did not clarify and make it more specific what the purpose of processing and the categories of personal data being collected and processed is actually necessary and proportionate. For instance, collecting location data without the knowledge of data subjects and not disabling this feature by default undermines the data minimization principle.

Accuracy

The principle of accuracy requires that the personal data be accurate and, where necessary, kept up to date. "Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay" (article 5 (1) (d) GDPR). According to the EDPB, the controller should consider this principle "*in relation to the risks and consequences of the concrete use of data.*"

¹⁵² Qualtrics, 'The Qualtrics' Cloud Security & Privacy Framework' (April 2025, Version 9.0).

¹⁵³ CJEU 4 October 2024, C-446/21 (Schrems vs Meta), para. 65.

As was stated throughout this DPIA, SURF was not able to get the full list of the Personal data must be accurate and linked to a specific purpose. Based on the DSAR responses, educational institutions are unable to clearly associate the personal data with its corresponding purpose and data subject categories. This limitation makes it more challenging to uphold the principle of accuracy in this context.

The risks to accuracy principle stems from the usage of the AI Response which SURF analysed in Section A.6.3.6. Since the AI Response Task uses an LLM, it is susceptible to hallucinations (generation persuading but possibly factually incorrect information). The accuracy principle from Article 5 (1) (d) GDPR 'reasonable steps' should be taken to rectify or erase the inaccuracy, therefore it has been interpreted as an obligation of means, not one of results.¹⁵⁴ Qualtrics, as a processor, is obliged to assist the controllers in providing correct data in accordance with accuracy principle.¹⁵⁵

Storage limitation

The principle of storage limitation requires that personal data should only be kept for as long as necessary for the purpose for which the data are processed. Data must *'not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed'* (Article 5(1)(e), first sentence, GDPR). This principle therefore requires that personal data be deleted as soon as they are no longer necessary to achieve the purpose pursued by the controller. The text of this provision further clarifies that *'personal data may be kept longer in so far as the personal data are processed solely for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1), subject to the implementation of appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject'* (Article 5(1)(e), second sentence, GDPR).

Additionally, "The Controller may determine the duration of personal data being processed by Processor. The Processor will store personal data no longer than necessary to provide the services requested by the Controller."

During SURF's DPIA, one of the key objectives was to identify the expected retention period for the different categories of personal data or, the criteria for determining that period. This information was not provided. The information on storage limitation, was determined from the Qualtrics 'Data Retention' document.¹⁵⁶ Qualtrics mentioned that: *'data retention periods are determined by the institutions, therefore we cannot provide this information on their behalf.'*¹⁵⁷

Integrity and confidentiality

Personal data must be processed in such a way as to ensure its appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (Article 5(1)(f) GDPR together with Article 32(1) and (2) GDPR).

¹⁵⁴ De Bot, *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context*, p. 497

¹⁵⁵ Article 28 GDPR.

¹⁵⁶ Qualtrics, 'Data Retention' (Qualtrics Support) <https://www.qualtrics.com/support/survey-platform/sp-administration/data-privacy-tab/data-retention/> accessed 30 July 2025.

¹⁵⁷ Qualtrics feedback from the 21st of February 2026.



Subsidiarity

A subsidiarity assessment within a DPIA evaluates whether a specific, less-intrusive method can achieve the same processing goal, ensuring data processing is necessary. This will depend on whether institutions already use other means for the use cases within the scope of this DPIA for Qualtrics XM. The assessment of whether other survey platforms are less intrusive must be done by comparing the DPIAs on other services.

¹⁵⁸ SOC 2 Report Qualtrics Report on Qualtrics' System and Organization Controls Relevant to Security, Availability, and Confidentiality, November 1, 2024 to October 31, 2025.

B.5 Data Subject Rights

The GDPR grants data subjects several rights, including the right to information, access, rectification, erasure, objection to profiling, data portability, and the right to lodge a complaint. It is the responsibility of the data controller (such as a Dutch educational institution) to provide this information and respond to these requests accurately and within the required timeframe.

When the data controller engages a data processor, such as Qualtrics, the GDPR requires that the data processing agreement explicitly states that the processor will assist the controller in fulfilling these obligations related to data subject rights.

Qualtrics explains in its Privacy Policy, that an individual has the right to exercise data subject rights in relation to personal data for which Qualtrics acts as a data controller. Qualtrics states that it is a processor for the Customer Data. Qualtrics as a processor is contractually obligated to immediately inform the data controller that they received the request, and then assist the controller in fulfilling it. The controller remains responsible for the overall response to the data subject. However, the controller should receive the assistance from Qualtrics to provide a data subject with a necessary information.

B.5.1 Right to information

Data subjects have a right to information (Articles 12-14 GDPR). This means that data controllers must provide people with easily accessible, comprehensible and concise information in clear language about, inter alia, their identity as data controller, the purposes of the data processing, the intended duration of the storage and the rights of data subjects.

The DPA is incomplete and lacks the necessary specificity regarding the processing activities, purposes, and categories of personal data processed by Qualtrics. As a result, SURF was unable to clearly distinguish between the data processing activities carried out on behalf of the data controller and those for which Qualtrics independently determines the purposes and means of processing.

This lack of clarity undermines the institutions' ability to fully comply with its transparency and accountability obligations under the GDPR. Furthermore, the unclear allocation of purposes for which personal data is processed and the blurred division of responsibilities between the institution and Qualtrics, makes it difficult for either party to effectively and accurately fulfill their information obligations under the GDPR.

B.5.2 The right to access data

The first fundamental right is the right to access. Data subjects have a (fundamental) right to access personal data concerning them. Upon request, data controllers must inform data subjects whether they are processing personal data about them (directly, or through a data processor). If this is the case, they must provide data subjects with a copy of the personal data processed, together with information about the purposes of processing, recipients to whom the data have been transmitted, the retention period(s), and information on their further rights as data subjects, such as filing a complaint with the Data Protection Authority.

Qualtrics as a data processor, should assist data controllers with providing data subjects with the right to obtain access to the personal data Qualtrics holds about them. This can be done through the Export Response Data: *'The exported data can be shared with the data subject in multiple formats, such as CSV, XML, SPSS, and others, ensuring compliance with the access request in a usable and transparent manner.'*¹⁵⁹ However, when SURF submitted the DSAR, the foundational information about the purposes, the categories of data subjects, personal data, retention periods was not included.

B.5.3 Right to rectification

Data subjects have the right to rectify inaccurate or incomplete personal data (Article 16 GDPR). Qualtrics offers instructions to Customers and data subjects how to modify or correct personal data within the XM platform.¹⁶⁰ Only authorised users (Brand Administrators) are allowed to edit submitted responses.

B.5.4 Data Deletion (Right to erasure)

Under Article 17 of the GDPR, data subjects have the right to erasure of their personal data in certain cases, such as when it is no longer needed, consent is withdrawn, or processing is unlawful.

If a data subject requests deletion of their personal data, Qualtrics offers guidelines to their page on the Right to Erasure.¹⁶¹ Data can be deleted in various ways depending on the type and location such as survey responses, XM Directory, and dashboards.

Qualtrics backs up data for disaster recovery, but users are responsible for their own backups and retention policies. Once data is deleted, all related backups will be removed within 90 days.

Since Qualtrics might process sensitive data such as bsn, the data should not be left after the request to delete the data. Because the bsn makes it easier for government organisations to exchange personal details without making errors, therefore this number is connected to all the information that the government can have about an individual. It is a sensitive identifier that can be used in various types of fraud, including identity theft and phishing scams. Therefore, controllers and processors need to make sure that this data will not 'reappear' in the system again. SURF has not received evidence or additional documentation about the process deletion. Therefore, SURF cannot confirm the exercise of the right to erasure further.

¹⁵⁹ Qualtrics, 'Export Formats' (Qualtrics Support) <https://www.qualtrics.com/support/survey-platform/data-and-analysis-module/data/download-data/export-formats/> accessed 10 October 2025.

¹⁶⁰ Qualtrics, 'Qualtrics GDPR Compliance – Data Modification' (Qualtrics Support) <https://www.qualtrics.com/support/survey-platform/getting-started/qualtrics-gdpr-compliance/#DataModification> accessed 10 October 2025.

¹⁶¹ Qualtrics, 'Right to Erasure' (Qualtrics Support) <https://www.qualtrics.com/support/survey-platform/sp-administration/data-privacy-tab/right-to-erasure/> accessed 10 October 2025.

Part C Description and Assessment of Risks to Data Subjects

C.1 Introduction

Before examining the details of the risk classification, it is important to mention that Qualtrics did not provide clear explanations or sufficiently address the questions raised. The 'black box' approach was taken in this DPIA. This is why some of the risks were classified as high, because no sufficient information from Qualtrics was provided to conduct a balanced DPIA. The absence of transparency and cooperation from Qualtrics hindered the research from achieving a more collaborative and well-informed outcome.

C.1.1 Identification of risks

Below, a general distinction is made between the risks of the processing of metadata on the one hand, and the Content Data on the other hand. Subsequently, 11 specific data protection risks are described, of which 7 relate to the processing of Diagnostic Data, and 4 to the Content Data. Generally speaking, data protection risks can appear in the following categories:

- inability to exercise rights (including but not limited to privacy rights)
- inability to access services or opportunities
- loss of control over the use of personal data
- discrimination
- identity theft or fraud
- financial loss
- reputational damage
- physical harm
- loss of confidentiality
- re-identification of pseudonymised data or
- any other significant economic or social disadvantage.¹⁶²

C.1.2 Classification of the risks

A risk matrix is used to visually represent and classify the factors of probability and impact. SURF uses the Information Commissioner's Office ('ICO') matrix.¹⁶³

The risk matrix consists of a table with two axes, one on the left and one on the right, with the probability of occurrence on the horizontal axis and the impact on the vertical axis.

¹⁶² Information Commissioner's Office, *Overview of data protection harms and the ICO's taxonomy* (Version 1, April 2022) <https://ico.org.uk/media2/about-the-ico/documents/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf> accessed 10 April 2026.

¹⁶³ Information Commissioner's Office, *How do we do a DPIA?* <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/> accessed 10 April 2026.

Impact of the damage	Heavy impact	Low risk	High Risk	High risk
	Medium impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Low probability	Reasonable chance	High probability
	Chance of damage occurring			

Figure 14 Risk Matrix

C.2 Risks to Data Subjects

This part concerns the description and assessment of the risks for data subjects. This part starts with an overall identification of the risks to the rights and freedoms of data subjects as a result of the processing of the Customer personal data and metadata (including purposes of the processing of the corresponding personal data). The risks will subsequently be classified according to the likelihood they might occur, and the impact on the rights and freedoms of the data subjects when they do.

C.2.1 Loss of control – Contractual role determination (Low)

The DPA with Educational institutions through a reseller [REDACTED] is not a DPA concluded between an educational institution and Qualtrics, but rather through a reseller. The DPA established that both a vendor and reseller are processors. This creates an ambiguity in role allocation and increases misunderstanding of what responsibilities Qualtrics and [REDACTED] as processors have. However, [REDACTED] cannot be a processor because [REDACTED] is not a platform vendor, but a reseller. The basis of this risk was explained in the section on Contractual context and role determination.

The ambiguity of the role allocation increases the likelihood of unlawful processing due to possible lack of clear responsibilities. Mentioning that both the vendor and reseller are processors is not reasonable and hinders the direct contractual link between the actual processor (Qualtrics) and the controller (educational institutions). For example, if the educational institution submits a GDPR-related request directly to Qualtrics, the assumption (stemming from the DPA) could be that such information can also be provided by the reseller. However, in practice, the reseller does not have this information. This disconnect between contractual rights and operational reality stemming from the documentation gaps of mistakenly naming a reseller to be a processor. Therefore, the impact is high.

The likelihood for the operational failures is low because the number of institutions is minor and education institutions are able to amend the role of the reseller [REDACTED] in the DPA. Otherwise controllers might wrongly assume they can rely on the reseller to enforce GDPR rights such as data subject requests due to indirect contractual link.

Therefore, the risk of the ambiguous role determination is low. Education institutions either should amend existing agreements and state that only Qualtrics is a processor, or have a direct contractual agreement to mitigate this risk affecting the data subjects.

C.2.2 Loss of control – data agnostic approach undermining the parties’ role allocation and purpose limitation principle (High)

There are existing documentation gaps that were observed during the review of the documentation that related to the Qualtrics XM services. Initially in the DPIA process, Qualtrics refused to share more information than what was publicly available or through the Trust Centre, which was not sufficient to fill in the gaps of the missing information or insufficient documentation in public documentations such as Privacy policy, GTC, and requested documentation from educational institutions such as DPA.

Additionally, in the section on Qualtrics’ Purposes as a Controller, SURF mentioned that according to these 7 purposes Qualtrics acts as a controller (according to the Privacy Policy):

- 1) To provide the services;
- 2) To communicate with the client about the services;
- 3) To improve, monitor, personalise, and protect the services;
- 4) For research and development;
- 5) For marketing and advertising;
- 6) For compliance and protection;
- 7) To train artificial intelligence tools.

Qualtrics acts both as a processor (on behalf of institutions) and as a controller (for its own purposes, such as analytics and AI training). However, Qualtrics also processes personal data that falls under the DPA for their own purposes for the service development such as LLM training. Unauthorised processing of personal data for the vendor’s own purposes can create a high impact on data subjects. If Qualtrics reuses the personal data for its own purposes without a lawful basis, this violates the purpose limitation principle. SURF found out that personal data might be used to train AI tools.¹⁶⁴ In order to check if the purposes match the purposes reflected in the DPA and other agreements, a list of personal data and categories of personal data matching the relevant purpose should be mentioned in the Schedule 1 of the DPA to provide a clear and transparent overview of data processing activities.

In such setups, categorisation of data is often blurred or incomplete, especially when not clearly separated in contracts or privacy notices. Qualtrics provided the types of Personal data (the subset of Customer Data) that are usually defined by the customer. This data was incorporated into the Table 5 Personal data mapping for Qualtrics as a processor. During the technical research, SURF observed that Qualtrics processes the data further for the development purposes when personal data is de-identified and aggregated. Qualtrics states that it maintains a clear separation between its roles as processor and controller.¹⁶⁵

The likelihood of damage occurring is high because no information is provided to SURF about processing purposes, legal bases for processing, categories of data and data subjects, and data retention criteria. Without this clarity of the specific and lawful purpose, and inadequate

¹⁶⁴ <https://www.qualtrics.com/privacy-statement/>

¹⁶⁵ Qualtrics response to SURF from the 9th December 2025.

documentation, the risk of not being able to provide clear, complete processing document for noncompliance is high.

SURF realises that the vendor implements a data agnostic approach, and acts on behalf of the instructions of the education institutions (their customers). However, without mapping the purposes to the categories of personal data in the Schedule 1 of the DPA, it is more complex for education institutions to verify their internal purposes are aligned with those contractually agreed upon. This increases the chance that data is processed inconsistently with the agreements with educational institutions.

The impact in this situation is high because it is non-compliance with the core GDPR principles according to Article 5 (1) GDPR. Even though SURF categorised the available categories of personal data processed by Qualtrics in the role of data controller (See Table 4), Qualtrics did not provide the full overview of the personal data processed on behalf of the Customers. Therefore, the lack to demonstrate that Qualtrics complies with the core GDPR principles can erode trust within educational institutions, and affect the fundamental rights of data subjects.

C.2.3 Inability to exercise data subjects rights – Transparency issue with the DSAR support to institutions. (High)

According to the GDPR requirements, data subjects must be informed about the categories of personal data collected, the purposes and the retention periods. If there is no an adequate support to educational institutions, a vendor might hinder the right to access data (Article 13 and 14 GDPR).

In the initial stages of our technical research, SURF observed that access to personal data through the platform's user interface is limited to survey response data, excluding critical system-generated data, user account metadata, error logs, or access records. Additionally, the vendor refuses to assist directly with DSARs for data processed on behalf of the institution, and instead refers users to a generic self-service support page. This page only covers manual export of respondent survey data, offering no support for accessing broader personal data processed by the system.

Qualtrics describes this approach because of the Controller's responsibility in providing its data subjects with the DSAR:

*'Controller Responsibility for DSARs: Under the DPA, if Qualtrics receives a request from a Data Subject relating to Personal Data, Qualtrics is obligated to promptly notify the Customer and will not respond to the request itself. Instead, Qualtrics asks the Data Subject to redirect the request to the Customer. This is because the Customer, as the Controller, has the direct relationship with the data subjects and solely determines the purposes and means of processing.'*¹⁶⁶

Therefore, the responsibility is on the Customer to provide the full response to the DSAR. This corresponds to the vendor's choice of being a data agnostic platform. However, data subjects

¹⁶⁶ Qualtrics response to the SURF question from the 9th December 2025.

have the right of obtaining the 'copy' of a personal data meaning that the data subject must be given a faithful and intelligible reproduction of all those data.¹⁶⁷

Qualtrics operates a DSAR tool described in the Section Personal Data Request tool. This new DSAR export tool provides the firstly missing information, but still misses the logging information.

The impact of providing insufficient information to customers on data subjects is high, because fundamental rights of the Customers' data subjects are at stake. No full information was provided by Qualtrics in the beginning, and educational institutions could not fulfill their controller's obligation to provide a data subject with a full disclosure either.

The likelihood of the risk occurring is high, because the probability that data subjects get the DSAR missing the logging data, or incomplete disclosure about data processing such as anonymisation techniques used by Qualtrics and LLM training, makes the data subject rights non-exercisable by data subjects.

Overall, the risk is high.

C.2.4 Lack of transparency in the subprocessor list – Incomplete subprocessor list (High)

During the technical research some additional services were discovered such as Google Analytics (Google LLC), Pendo, Amplitude. These subprocessors were either incompletely described or entirely absent from the official subprocessor list. Since Qualtrics does not provide sufficient information about its data processing activities which are considered confidential by a vendor, not being able to inform its users about the actual third party processing personal data creates legal and operational risks for educational institutions. SURF provided the evidence in the Section Technical Investigation of Data Flows and Endpoints about more parties being involved in data processing activities than included in the Qualtrics' subprocessor list.¹⁶⁸

The impact is high because under GDPR, data processors must inform controllers about third-party processors involved in data processing. Indeed, Qualtrics informs users about new subprocessors through sharing the email notification to the customers, however they are not mentioned in the subprocessors list. The likelihood is high because endpoint testing during platform use revealed frequent connections to domains associated with Google Analytics, Pendo, Amplitude, all of which are not transparently listed in the vendor's official subprocessor documentation. Therefore, the risk is high.

C.2.5 Lack of transparency for the optional subprocessor Imperium LLC (No longer a risk)

Qualtrics may engage Imperium, LLC, a US-based optional subprocessor, to perform device fingerprinting and fraud detection through the collection of metadata such as IP address, browser/device info, and bot detection scores. This constitutes profiling and fingerprinting. However, it is unclear when and how Imperium is actually activated, as there is no visibility

¹⁶⁷ Case C-487/21, Österreichische Datenschutzbehörde and CRIF.

¹⁶⁸ Qualtrics, 'Subprocessor List' (Qualtrics, n.d.) <https://www.qualtrics.com/subprocessor-list/> accessed 14 April 2026.

provided to Brand Administrators or researchers regarding its usage on specific responses. Also, there is no clear audit trail or logs confirm if metadata is processed by Imperium.

This creates a transparency and accountability gap in the processing of personal data via third parties.

Under Recital 30 GDPR, metadata like device characteristics, IP addresses, and browser signatures may be used for fingerprinting, and are considered personal data. This type of profiling can: infringe on users' privacy rights, trigger the need for explicit consent in some jurisdictions (especially under ePrivacy and for cookie-like technologies), require detailed transparency in privacy policy. Therefore, the impact on data subjects can be detrimental since Qualtrics uses online identifiers.

There is a reasonable chance because even though Imperium LLC is labeled 'optional', the lack of a clear opt-in or opt-out mechanism creates a situation where its processing may be active by default or indirectly triggered. Therefore, it is probable that this subprocessor might be switched on in certain conditions without the controller's or user's awareness.

Given the impact and the likelihood of occurrence of this risk, it was classified as high.

However, due to the fact that Qualtrics stopped using Imperium LLC, this risk is no longer applicable to this DPIA. Additionally, Qualtrics is advised to remove this subprocessor from the list of subprocessors.¹⁶⁹

C.2.6 Lack of transparency – transparency report (High)

Qualtrics does not publish transparency reports about government requests. Qualtrics stated that it does not publish transparency reports about government requests publicly. Moreover, in the DPA it is stated that Qualtrics may process personal data if required so by applicable law and Qualtrics notifies the Customer of that legal requirement. However, this approach lacks transparency regarding the number of government requests that Qualtrics receives, specifically about the frequency of government data requests, the types of requests (national security, law enforcement), whether requests were complied with or rejected, and whether data of EU citizens was involved. According to Article 13 and 14 of the GDPR, the controllers (education institutions) should provide data subjects with the information regarding personal data collected from the data subjects.

There is an obligation on the intermediary services (which include online platforms) to provide transparency reports regarding their content moderation activities according to the Digital Services Act ('DSA').¹⁷⁰ This requirement includes providing annual reporting which is publicly available and easily accessible. The information shall include Government orders such as the number of orders received from the government authorities. The DSA provides more specific obligation, and represents the recognized risk of the information gap between platform and the data subjects.

¹⁶⁹ Qualtrics, 'Subprocessor List' (Qualtrics, n.d.) <https://www.qualtrics.com/subprocessor-list/> accessed 14 April 2026.

¹⁷⁰ Article 15 Digital Services Act ('DSA')

Qualtrics' position and contractual commitments are:

- *SCC-Specific Report: Qualtrics will make available to the Customer on a yearly basis a report containing statistical information on any requests from intelligence authorities for the disclosure of personal data transferred on the basis of the Standard Contractual Clauses (SCCs).*
- *Content of the Report: This specific report lists the number of such requests received in a given calendar year.*¹⁷¹

Despite providing the report to the Customers, the lack of transparency for data subjects creates an information gap for data subjects. It has a high impact on data subjects. Data subjects should receive the because end users should be able to receive this information publicly, and not only for the vendor to provide a *'compliance mechanism for the contracting Customer to facilitate their oversight under international data transfer requirements'*¹⁷² which does not contribute to a better transparency mechanism to inform the data subjects about the government requests.

The likelihood of the risk occurring is high, because there is a chance that data subjects remain uninformed. From a processor accountability perspective, Qualtrics has designed this mechanism to correspond to its own contractual and legal obligations towards the Customers, and not the data subjects. Therefore, education institutions, as controllers, need to proactively inform data subjects through privacy notices and transparency reports based on the Qualtrics' SCC-Specific Report. In practice, education institutions refer to the Qualtrics' public available information. This excludes the details about the information collected from the data subjects, because Qualtrics shares it with the Customers only.

The lack of transparency (regarding with who, when and why the data subjects' information was shared with government authorities) and effect on processing of personal data has a high impact on data subjects. There should be a clear communication how the controllers and processor (to assist the controller with sharing this information with data subjects) provide these details to the data subjects. The likelihood of the risk occurring to the data subject is significant because the chance that data subjects are not informed remains high. Education institutions may lower the likelihood of the risks by providing this information to the data subject. This risk is classified as high.

C.2.7 Lack of transparency – Proxy Login (High)

This feature is described in the Section Proxy Login. The end user receives no notification that a proxy login has occurred. The proxy functionality does not correspond to the GDPR's transparency obligation in two ways: at the point of access (the end user does not know their account is accessed in real time) and after the fact (no notification mechanism).

The impact on data subjects is high because everytime a Brand Administrator uses proxy login, the end user is unaware. This makes the impact of this risk high because the impersonator can view and/or access personal data which can potentially lead to the unauthorised data access. Since the user is not informed pre- or post-session, more measures should be implemented to

¹⁷¹ Qualtrics' responses to SURF questions from the 9th of December 2025.

¹⁷² Qualtrics' responses to SURF questions from the 9th of December 2025.

comply with transparency principle from Article 5 (1) (a) GDPR. This makes this feature a high risk for data subjects.

The likelihood of this risk is high due to the fact that the feature is available without any notification controls of the end-users. It is frequently used since it is a standard support tool.

C.2.8 Loss of control - internal system and performance logs (High)

During the SURF research, it was identified that Qualtrics maintains a log of internal system and performance events. From Qualtrics documentation, they are used for the purpose of capturing technical metrics related to infrastructure health, service integrity, and operational anomalies. Moreover, the logs contain metadata such as the IP address of the requestor, the protocol used, and other information mentioned in the Section Internal System and Performance Logs. SURF identified that these internal logs are not made available to the customers. Only a limited subset of activity data is surfaced to customers via the platform's user interface or API endpoints.

From the perspective of impact, educational institutions will not be able to track the processing of personal data, and as a consequence will lose the track of the exact personal data which is processed by Qualtrics either in the role of controller and processor. As a result, even though the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR according to Article 24, educational institutions will not have the full control of what whether the metadata is included in the data processing at the level of performance logs and will not be able to inform their data subjects about this processing.

Likelihood of the damage occurring is high, because Qualtrics isn't providing access to the personal data in these logs at this moment.

Therefore, the risk is classified as high.

C.2.9 Loss of control: Reidentification of pseudonymised data – anonymisation techniques to train AI models (High)

SURF experienced the lack of transparency regarding the use of 'proprietary rules' and reliance on machine learning techniques for anonymisation. Qualtrics' lack of full auditability and the potential for advanced re-identification attacks cause an overreliance on Qualtrics' internal processes. If the information about the internal processes was more available, the risk would be minimised because Qualtrics will be able to show education institutions that the vendor is compliant with the GDPR and does not have any high data processing risks.

The impact on data subjects is high because sensitive personal data (such as Dutch specific identifiers) could be exposed by using advanced inference techniques if re-identification occurs.

Qualtrics has provided SURF with [REDACTED] where anonymisation techniques and methods are demonstrated.

Qualtrics mentioned few personal data categories which are flagged and anonymised/reduced. This excludes entirely Special types of personal data, as well as other sensitive information.

Qualtrics mentioned this list is not reviewed by legal specialists, but only technical experts of the vendor.

Additionally, Qualtrics does not have any anonymisation accuracy metrics for Dutch, and also could not share with SURF if the model has been trained on Dutch at all. Therefore, how the anonymisation technique work with Dutch remains unclear. Regarding the 'human in the loop', no actual metrics were shared.

Additionally, a related aspect to the risk of reidentification is that SURF could not verify in the Qualtrics' documentation what types of AI models Qualtrics uses, there are no published metrics on any of the Qualtrics' AI. Therefore, it is complex to verify the effective anonymisation techniques to train AI models. Although, in SURF's experience, vendors do provide this information to determine the effectiveness of the anonymisation techniques.

The likelihood of this risk occurring increases when anonymisation techniques are not clearly checked for the compliance of anonymisation techniques. Lack of transparency reduces the ability of SURF and education institutions (data controllers) to assess risks and compensating controls which significantly impacts data subjects. This marks the likelihood high. SURF in its conclusions cannot overrely on Qualtrics' internal processes.

The chance of damage occurring is high because data subjects are not aware of certain data processing activities. In the Section Anonymisation and Pseudonymisation, SURF shared the findings of the technical research. Performance metrics do not correspond to the same level of details as vendors are providing during the DPIAs.

Given that SURF has limited visibility into Qualtrics' internal processes and the likelihood of the risk is high as long as transparency is lacking, this risk is qualified as high.

C.2.10 Loss of Control- Inadequate support for transparent user communication and informed consent (High)

The risk here is that Qualtrics provides only a minimal default disclaimer, placing the full responsibility on educational institutions (as data controllers) to: inform users properly about data collection, use retention, and rights; obtain valid informed consent, and comply with transparency obligations.

For example, Qualtrics' cookie consent banner lacks a 'Reject All' option, effectively nudging users toward data acceptance and complicating the opt-out process. More critically, the platform deploys cookies immediately upon loading the main page, before a user choice is made. Therefore, data subjects are unable to prevent the processing of their behavioral data, leading to a direct violation of the ePrivacy Directive and GDPR transparency requirements.

Impact is high, because an invalid consent may be obtained if notices are unclear about data retention periods and legal basis for the data processing. The likelihood of the risk would be high because institutions as data controllers rely on Qualtrics as data processor and its default. Overall, the risk of inadequate support for transparent user communication and informed consent is high.

C.2.11 Loss of control – Consent banner and Location information (High)

A critical aspect is the allocation of responsibility regarding the placement of the consent banner and informing data subjects about the collection of location information. Qualtrics adopts a firm stance that, as a data processor, they do not interact directly with data subjects regarding these technical collections. Consequently, the legal obligation to provide notice and obtain valid consent rests entirely with the institution (the controller).

The description to this format is that this is a hidden question that captures browser and operating system information. During the technical research, SURF observed that location data was collected which is not described to the users in a clear and concrete way. This approach does not follow data minimisation principle. The collection of IP addresses, location information is enabled by default, and administrators should do it by themselves. Additionally, the consent banner is provided by the researchers which may not include all processing activities.

The impact on data subjects is high because they will not be aware of what data is processed when the survey is being filled in, and why would the IP address of the end users be collected and for what purposes. The likelihood of this risk occurring is high because this is a built-in feature which results in collecting more personal data than they have legally disclosed and does not correspond to the Privacy by Design choices. Overall, this risk is classified as high.

C.2.12 Inadequate evidence of the Brand Deletion Requests (Resolved)

SURF confirmed that Qualtrics holds third-party certification such as ISO 27001, SOC2 that provide reasonable assurance in its security controls.

[REDACTED]

[REDACTED]

[REDACTED]

¹⁷³ Qualtrics responses to the SURF questions from the 9th of December 2025.

Likelihood of the risk occurring is remote, [REDACTED], which was previously identified, no longer appears in the most recent SOC2 Report.¹⁷⁴ It is important to note that remediation of the control does not retrospectively answer the outstanding questions surrounding the period during which the control failed. Specifically, what occurred, which data subjects or systems were affected, and for how long the deficiency persisted. Those questions remain relevant from a GDPR accountability and incident management perspective and should continue to be addressed separately.

Regarding the current risk position: Qualtrics' new SOC 2 report returns a positive outcome, and the remediation letter provided by Qualtrics sets out concrete countermeasures designed to prevent recurrence of the issue. The unresolved questions about the failure period mean that accountability for that period cannot be demonstrated. Taking these factors into account, the risk associated with [REDACTED] is resolved. However, the risk remains in the internal processes of the vendor for not being able to present the [REDACTED]. This risk stems from vendor's choice for the level of transparency and accuracy regarding its data processing activities.

C.2.13 Loss of Control - Incomplete automated detection by ExpertReview of specific sensitive identifiers for Dutch education customers (High)

Sensitive data policy primary feature is to protect respondent privacy by identifying and preventing the collection of sensitive data. Personal data is automatically blocked and redacted through the functionality of ExpertReview. Qualtrics is a data processor, and the Brand Administrator of the educational institution defines specific Sensitive Data Policies by setting up topics and requirements. However, the current system does not automatically detect Dutch-specific sensitive identifiers. For example, Dutch mobile phone numbers and Dutch BSN (burgerservicenummer). These identifiers may therefore be collected without triggering alerts or redactions.

Brand administrators can manually create custom detection rules, however the impact of this feature not being specific to Dutch educational institutions has a high privacy impact. Because Dutch bsn is considered sensitive personal data under GDPR. If this data is not redacted, failure to detect these identifiers may lead to unlawful processing and breach with data minimisation principles.

The likelihood depends on whether education institutions actively configure personal data through the ExpertReview. This function includes a disclaimer that it does not warrant any users from any data specific languages. The tool will not be able to detect any Dutch specific configurations such as BSN. Although education institutions code their own rules and ensure that it functions in accordance with the set rules, the likelihood that the risk will occur when institutions use this feature is more likely than not. Because even if this feature is not used actively by the institutions, there is a significant possibility that certain groups of data subjects that use the feature may be significantly impacted.

¹⁷⁴ Qualtrics SOC 2 Type 2 Report on Qualtrics' System and Organization Controls Relevant to Security, Availability, and Confidentiality (February 2026).

Therefore, the classification of the risk is high.

C.2.14 Lack of transparency – no publication of accuracy metrics for Sensitive Data Policy and absence of feedback mechanisms (High)

The absence of published accuracy metrics for Sensitive Data Policy detection undermines educational institutions' ability to assess and manage risks about the system's reliability. As the result, educational institutions are unable to assess situation if sensitive data was not detected and thus exposed, or sensitive data being incorrectly flagged or redacted. This situation becomes more challenging with the absence of feedback and complaint processes to report detection inaccuracies.

The impact of this risk is high because it may cause educational institutions to struggle with demonstrating data accuracy and effective data minimisation without evidence of accurate or non-accurate detection mechanism.

The potentially high likelihood, complexity of sensitive data detection without published metrics, educational institutions must assume a moderate chance of detection errors. The lack of feedback means that errors may be left unchecked for extended periods.

The combination of high impact and high likelihood given the sensitivity of personal data, makes it a high risk to data protection.

C.2.15 Loss of control and lack of transparency – Insufficient control of translated user surveys Google Translate and Amazon Translate (High)

The platform Qualtrics XM automatically sends content to the external providers of translation function (Google Translate or Amazon Translate) without the possibility for Brand Administrators to disable this behaviour. Initially, Qualtrics did not inform users when content in the Data Analysis module has been processed in this way, nor has it disclaimers about possible translation inaccuracies.

The risk associated with the usage of third-party translation provides increases the risk of data exposure because the text is transmitted to external servers providers. Extra points are added where data could be intercepted. Brand administrators have no control to disable this data sharing. As the result, educational institutions cannot prevent potentially sensitive data from being sent out by default. Additionally, according to the section Translation Services, end users should manually enable the automatic translation by other translation services.

Qualtrics allows for the manual renaming of translation columns; however, this currently requires the user to append identifiers ('AI-translated to EN') to the field manually. This measure makes the likelihood of the risk occurring low if education institutions amend the identifiers.

The likelihood of automatic translation service depends on the frequency of the usage of this function, whether a researcher clicks the translate button. The likelihood increases with the more frequency surveys with sensitive content are translated. Frequent usage of Google Translate and Amazon Translate means that data exposure is recurring, but moderate. The

chance of damage occurring is medium risk because it depends how often data subjects are using the translation.

The impact on data subjects is high because there is loss of control over the accuracy of the processing of personal data.

C.2.16 Transfer outside of the EU/EEA - Automatic use of Google Translate and Amazon Translate (High)

This risk concerns the loss of sovereignty over the processes mentioned in the previous section.

The impact on data subjects is high because their personal data is transmitted to US-based hyperscalers (Google or Amazon) without the explicit consent of the subject or the intervention of the Controller (the Educational Institution).

The chance of damage is considered medium because it is triggered only when a researcher actively engages the 'Translate' function in the Data Analysis module. However, because the Brand Administrator cannot disable this feature globally, the institution cannot prevent an individual researcher from accidentally or intentionally triggering a non-compliant transfer.

Overall, this risk is classified as high.

C.2.17 Lack of transparency and absence of consent due to the incomplete cookie information (High)

In the section Technical Testing of Cookies, SURF explained that cookies that were not described in the Cookie policy were identified during the technical research. The description of some identified cookies was not included in the articles mentioned by Qualtrics. This lack of transparency limits the ability of educational institutions as data controllers to assess the cookies in use to provide or not provide an explicit consent.

SURF followed up on the 25 missing cookies that were encountered during the technical research. Qualtrics explained the purposes for cookies, however these purposes were not included in the Cookie statement. Additionally, the categories of personal data and the relevant subprocessors were also missing from this list.

The impact is high because educational institutions without knowing the purpose of the cookies collected and relevant personal data, may not demonstrate the compliance with the lawfulness of data processing. Under the ePrivacy Directive, cookies require the user's prior consent. Since no information on the cookies is presented, no valid consent is obtained. The likelihood is high, because it is occurring, and creates potential unlawful processing.

High impact and moderate likelihood makes this risk high for data subjects and causes unintentional compliance breaches for educational institutions.

Part D Description of Proposed Mitigation Measures

D.1 Mitigation Measures

The following section contains a table of the mitigating technical, organisational and legal measures that need to be taken by the education organisation or by Qualtrics to mitigate the identified 14 high risks and 1 low risks for the data subjects.

For each risk, the upper half of the table describes the current risk and shows the risk score from section C. The lower half of the table describes the measures that Xedule and the institutions can take and gives a score for the residual risk.

In the 'Dissenting opinion by Qualtrics', SURF shared the 'Suggested action by Qualtrics', where the vendor was given the space to provide their views about the mitigated measures for identified risks to the extent it considers efficient and feasible.

D.1.1 Loss of control – Contractual role determination

Loss of control – Contractual role determination						
Reference	Reason	Consequence	Chance	Impact	Risk Score	Current risk
Risk 1	Misalignment between legal documentation and the role of the reseller.	Education institutions may direct disputes to the reseller.	Low	Low	Low	
	Measures Institution	Measures Vendor	Chance	Impact	Risk score	
	Explicitly state in the DPA that data breach notifications shall be directed to the vendor from the education institutions.					
	SURF proposes to sign a direct DPA with Qualtrics.					
	If a direct DPA is not plausible or possible, add an addendum to the current agreement that Qualtrics is the sole processor. [REDACTED] should be stated as a 'reseller' or 'commercial intermediary'.				Low	

D.1.2 Loss of control – data agnostic approach undermining the parties’ role allocation and purpose limitation principle

Loss of control – data agnostic approach						
Reference	Reason	Consequence	Chance	Impact	Risk Score	
Risk 2	Data agnostic approach allows Qualtrics not to provide specific details on data processing.	The vendor prevents education institutions from verifying compliance with purpose limitation and data minimization.	High	High	High	Current risk
	Measures Institution	Measures Vendor	Chance	Impact	Risk score	
	Since the vendor will not provide categories, the institution must implement strict ‘data records’ for end-users such as researchers, staff or student. By limiting what fields can be created in the platform, the institution can ‘self-document’ the categories of data and data subjects.	Modular public page which includes specific information about the usual data categories processed and the mapped purposes to the personal data.			Low	
	Ensure that only the ‘informed’ core processing occurs.	Negotiate and provide education institutions an explicit ‘No-AI/LLM training based on the processing of Customer’s data’ in the DPA.				
	Prohibit the use of the platform for special categories of data.	Commit contractually to the absolute anonymisation (not just pseudonymization) for any data used for ‘Research and development’ or ‘Product improvement’. Give education institutions an option to opt out from the anonymisation processes.				
	Education institutions should have an explicit ‘No-AI/LLM training based on the processing of Customer’s data’.					
	Ensure that education institution’s own privacy notice explicitly lists the categories of personal data that vendor processes as a data processor and, possibly, as a data controller.	Map the categories of personal data which Qualtrics processes in accordance with 7 purposes for which Qualtrics acts as a data controller				
	In the Schedule 1, the categories of personal data should be mapped to the purposes.	Publish a public Data mapping for all Qualtrics products that list every possible category of personal data collected.				

		Provide a transparency dashboard for the admin to observe what exactly categories are being used, for example, for service development.				
--	--	---	--	--	--	--

D.1.3 Inability to exercise data subjects rights – Transparency issue with the DSAR support to institutions

Inability to exercise data subjects rights – Transparency issue with the DSAR support to institutions						
Reference	Reason	Consequence	Chance	Impact	Risk Score	Current risk
Risk 3	While survey responses are accessible, the logging information is missing.	With the DSAR tool being improved, the additional logging information may mitigate this risk.	Medium	High	High	
	Measures Institution	Measures Vendor	Chance	Impact	Risk score	
	When the DSAR misses certain categories of data, establish a formal procedure within the institution which includes sending a manual ticket to Qualtrics support specifically requesting the missing data.	Qualtrics should add the missing logging information and submit the full DSAR response to education institutions.			Low	
	Create a manual to end-users (admins, students, and others) about an updated DSAR tool.					

D.1.4 Lack of transparency in the subprocessor list – Incomplete subprocessor list

Lack of transparency in the subprocessor list – Incomplete subprocessor list						
Reference	Reason	Consequence	Chance	Impact	Risk Score	
Risk 4	The core of this risk is the undisclosed third-party processing.	Education institutions unknowingly transform data to entities that were not approved as subprocessors.	High	High	High	Current risk
	Measures Institution	Measures Vendor	Chance	Impact	Risk score	
	Request the information from the vendor about the full subprocessor list, and do it periodically within an education institution.	Add the mentioned subprocessors to the list of subprocessors.			Low	
	Disable the features associated with the third-party processing until the vendor adds a clear description of their purpose.	Provide opt-out which allows institutions to disable all third-party telemetry for the end-users.				

D.1.5 Lack of transparency reports

Lack of transparency reports						
Reference	Reason	Consequence	Chance	Impact	Risk Score	
Risk 6	The risk stems from the asymmetry of information between the vendor and the public.	Without public data on government requests, institutions cannot verify if the is subject to disproportionate surveillance, particularly by non-EU authorities.	High	High	High	Current risk
	Measures Institution	Measures Vendor	Chance	Impact	Risk score	
	While the specific Qualtrics report may be confidential, the institution can include a high-level statement in its own public transparency report. For example: <i>‘Our vendors have reported zero data disclosure requests from foreign intelligence authorities in the previous calendar year.’</i>	Launch a web page that provides aggregated, anonymized statistics on government requests globally. This should include: Number of requests received; Percentage of requests challenged or rejected; Categories of data requested.			Low	

D.1.6 Lack of transparency – Proxy login

Loss of control - internal system and performance logs						
Referen ce	Reason	Consequence	Chance	Impact	Risk Score	Curr ent risk
Risk 7	Proxy login enables Brand Administrators to access end-user accounts without the notification.	Unauthorised viewing of personal data of personal data may occur routinely and repeatedly without the data subject's knowledge.	High	High	High	
	Measures Institution	Measures Vendor	Chance	Impact	Risk score	
	Disable proxy login	Implement real-time end-user notification For example, it should be visible not only for the admin, but for the users who are being masqueraded on.			Low	
		Role-based limitations: restrict what an impersonator can access during a session.				

D.1.7 Loss of control - internal system and performance logs

Loss of control - internal system and performance logs						
Referen ce	Reason	Consequence	Chance	Impact	Risk Score	Curr ent risk
Risk 8	Qualtrics captures technical metrics and metadata in logs that are inaccessible to the Customer.	Because institutions cannot view, audit, or export these logs, they cannot 'demonstrate compliance' with data minimization or storage limitation principles for this specific dataset.	High	High	High	
	Measures Institution	Measures Vendor	Chance	Impact	Risk score	
	Explicitly mention in the DPA that performance logs are part of the data category in Schedule 1 of the DPA.	Publish a list for Customers that lists exactly what metadata is captured in performance logs.			Low	
		Provide the full copy of personal data (including the complete DSAR).				

D.1.8 Loss of control: Reidentification of pseudonymized data – anonymisation techniques to train AI models

Lack of transparency – anonymisation techniques to train AI models					
Referen ce	Reason	Consequence	Chanc e	Impac t	Risk Score
Risk 9	The risk conveys the black box approach to the anonymisation techniques used by the vendor.	Anonymised data is used for model training but provides no evidence of the accuracy or legal validity of these techniques, especially for the Dutch language.	High	High	High
	Measures Institution	Measures Vendor	Chanc e	Impac t	Risk score
	Insert a strict clause into the DPA stating that anonymisation and aggregation of institutional data for AI training or product improvement are strictly prohibited.	Qualtrics should publish a list of the data types its ML model is trained to detect.			Low
		Qualtrics should be more transparent about Dutch performance statistics. Be more transparent about Dutch performance statistics, explain thresholds and metrics for the human in the loop.			
		Explain and show the percentage/metrics of AI-anonymized data that is manually reviewed by human auditors.			
	Formally request a report on the metrics for Dutch-language. If the vendor cannot provide these, the institution should assume the anonymisation is technically insufficient.				
	Use the Brand Administrator settings to globally disable all generative AI features and automated insights until the vendor provides a transparency whitepaper that includes a list of all data fields being scrubbed.				

D.1.9 Loss of Control- Inadequate support for transparent user communication and informed consent

Inadequate support for transparent user communication and informed consent						
Referen ce	Reason	Consequence	Chance	Impact	Risk Score	Curr ent risk
Risk 10	Qualtrics' standard cookie banner typically lacks a 'Reject All' button on the first layer.	Education institutions unknowingly obtain 'invalid consent' from data subjects, making any subsequent data processing unlawful from the moment the page loads.	High	High	High	
	Measures Institution	Measures Vendor	Chance	Impact	Risk score	
	Build a dedicated consent form.	Update the global platform theme to include a 'Reject All' button as a standard feature, rather than requiring custom code from the Customer.			Low	
	Instruct researchers to add these consent forms and put it in if meta info is used (amongst any other questions that might reveal personal data).	Re-engineer the platform's entry point so that no non-essential cookies (analytics, functional preferences) are dropped until the consent API receives a positive signal from the user. (Qualtrics communicated to SURF that the vendor will investigate how to modify the entry point. No concrete commitments were provided).				

D.1.10 Loss of control – Consent banner and Location information

Loss of control – Meta info						
Referen ce	Reason	Consequence	Chanc e	Impac t	Risk Score	Curre nt risk
Risk 11	No consent banner and the collection of location information.	Education institutions unknowingly obtain ‘invalid consent’ from data subjects, making any subsequent data processing unlawful from the moment the page loads.	High	High	High	
	Measures Institution	Measures Vendor	Chanc e	Impac t	Risk score	
	Build a dedicated consent form.	Design the measure so non-essential cookies (analytics, functional preferences) are dropped until the consent API receives a positive signal from the user.			Low	
	Instruct researchers to build consent forms and inform the researchers about the proprocessing of location data being processed (amongst any other questions that might reveal personal data).					

D.1.11 Inadequate evidence of the Brand Deletion Requests (Resolved)

Inadequate evidence of the Brand Deletion Requests						
Reference	Reason	Consequence	Chance	Impact	Risk Score	Current risk
Risk 12	[REDACTED]	Creates a compliance gap that Qualtrics amended and demonstrated in early 2026.	Remote	High	Remote	
	Measures Institution	Measures Vendor	Chance	Impact	Risk score	
	Qualtrics indicated a new report would be available in early 2026. Institutions should formally request this document to verify [REDACTED] process has been tested and confirmed by independent auditors.	New SOC2 report is available.				

D.1.12 Loss of Control - Incomplete automated detection by ExpertReview of specific sensitive identifiers for Dutch education customers

Incomplete automated detection by ExpertReview of specific sensitive identifiers for Dutch education customers						
Reference	Reason	Consequence	Chance	Impact	Risk Score	Current risk
Risk 13	The 'Sensitive data policy' feature lacks pre-configured 'topics' for Dutch-specific identifiers, it fails to fulfill its purpose for institutions in the Netherlands.	Highly sensitive data, such as the BSN (Burgerservicenummer) or Dutch mobile numbers, can be collected without the system sounding an alarm.	High	High	High	
	Measures Institution	Measures Vendor	Chance	Impact	Risk score	
	Set the 'Sensitive data policy' to redact sensitive information from survey responses. This ensures that even if a respondent unprompted enters their BSN in an open-text field, the data is replaced with	Improve the Text iQ and ExpertReview to understand Dutch labels for sensitive data. For example, recognizing BSN will trigger for sensitive data warnings.			Low	

	asterisks or other substitute.					
	Do not actively configure personal data through the ExpertReview, until Qualtrics has carried out the measure described					

D.1.13 Lack of transparency – no publication of accuracy metrics for Sensitive Data Policy and absence of feedback mechanisms

Lack of transparency – no publication of accuracy metrics for Sensitive Data Policy and absence of feedback mechanisms						
Reference	Reason	Consequence	Chance	Impact	Risk Score	
Risk 14	The core issue is the lack of transparency regarding performance.	There is no feedback button within the survey-building interface. This creates the feedback gap for the institutions.	High	High	High	Current risk
	Measures Institution	Measures Vendor	Chance	Impact	Risk score	
	File tickets or support requests to Qualtrics for the feedback.	Qualtrics should participate in quarterly reviews to discuss known detection gaps and provide a roadmap for improving Dutch-specific identification together with SURF.			Low	
		Add a 'flag as inaccurate' button directly for the Sensitive Data Policy.				

D.1.14 Loss of control – Automatic use of Google Translate and Amazon Translate

Loss of control – Automatic use of Google Translate and Amazon Translate					
Reference	Reason	Consequence	Chance	Impact	Risk Score
Risk 15	Uncontrolled flow of data to subprocessors that are not managed directly by the institution's Brand Administrator.	The processing of data through automatic Google and Amazon translate indicate a data transfer.	Medium	High	High

	Measures Institution	Measures Vendor	Chance	Impact	Risk score	
	A manual action for the user who translates need to do (i.e. append 'AI translated to EN') to the field.	Qualtrics will provide a build-in feature for the institution to manually use the translate services.			Low	

D.1.15 Transfer outside of the EU/EEA - Automatic use of Google Translate and Amazon Translate

Lack of transparency and absence of consent due to the incomplete cookie information						
Reference	Reason	Consequence	Chance	Impact	Risk Score	
Risk 16	Uncontrolled flow of data to subprocessors based in the US that are not managed directly by the institution's Brand Administrator.	The processing of data through automatic Google and Amazon translate indicate a data transfer outside of the EU/EEA. .	Medium	High	High	Current risk
	Measures Institution	Measures Vendor	Chance	Impact	Risk score	
	Inform the end-users about the translation functionality.	Provide other option for translation: European alternatives. Provide an option for the brand administrators to add additional translation options manually.			Low	

D.1.16 Lack of transparency and absence of consent due to the incomplete cookie information

Lack of transparency and absence of consent due to the incomplete cookie information						
Reference	Reason	Consequence	Chance	Impact	Risk Score	
Risk 17	Without a complete and accurate cookie list, any consent obtained from a student or researcher is technically invalid, as they cannot be 'informed' about tracking they do not know exists.	Data subjects will not be aware for the processing activities.	High	High	High	Current risk
	Measures Institution	Measures Vendor	Chance	Impact	Risk score	
	Issue a formal instruction to the vendor to deactivate any cookies identified as 'Marketing' or	Qualtrics should provide a real-time, machine-readable list of all cookies currently in use. This would allow educational institutions to automatically update their own transparency notices whenever the vendor adds a new tracker.			Low	

	'Targeting' that are not strictly necessary for the service.					
		For every cookie used, Qualtrics must provide a clear technical justification proving it is 'Strictly necessary' under Article 5(3) of the ePrivacy Directive.				

Conclusion

This DPIA identified 14 high and 1 low risks associated with the use of Qualtrics Design XM for Education. The mitigating measures proposed in Part D by SURF, education institutions may view the measures that SURF suggested to mitigate some of the risks. These measures correspond to low risks and features that may be disabled by the institutions. The high risks are unlikely to be resolved without firm and concrete commitments from Qualtrics to implement appropriate technical and organisational measures at the vendor level.

Throughout the DPIA process, SURF constantly sought the best possible outcome of the DPIA, and engaged with Qualtrics at every stage of the project. While Qualtrics was not actively involved in the initial stages of the assessment, its review of the completed DPIA and identified risks led to a recognition of the value of more substantive participation. The vendor has not committed to implementing mitigating measures and has disputed the SURF's risk classification.

The high risks identified concern the following: the data agnostic approach, incomplete list of subprocessors, loss of control and transparency due to the incomplete consent collection, incomplete cookie lists, and incomplete handling of the DSARs.

SURF's objective is to ensure that the use of Qualtrics' products by education customers within the Netherlands is fully compliant with the GDPR. As SURF is at the forefront of conducting and publishing DPIA outcomes on behalf of its members. Given the unresolved high risks identified, SURF urges education institutions to carefully consider the findings of this DPIA before continuing using Qualtrics' platform.

Should Qualtrics provide firm commitments to implement the necessary mitigating measures, SURF will update this assessment accordingly.

Appendix 1 Technical Testing Scenarios

This appendix describes the testing scenarios that were executed for data flow analysis, how they were performed, and what they tested, alongside the setup for executing the scenarios.

1.1 Testing Software and Hardware

In conducting man-in-the-middle (MITM) data flow gathering, a stable and reproducible test environment is critical. We tested Qualtrics on a desktop computer. This section outlines the software and hardware used at the time of testing.

For intercepting HTTP(S) traffic, we used mitmproxy. mitmproxy allows us to intercept both local traffic generated on the machine, as well as external devices by hosting a proxy server. mitmproxy ran on the following machine:

- Apple MacBook Pro 2023 14", M3 Pro (11-core CPU, 14-core GPU, 18GB RAM)
- macOS Sequoia 15.5
- mitmproxy 12.1.1

For testing the web-based Qualtrics platform, we used Google Chrome v138.0.7204.101, which ran on the aforementioned machine (local traffic). Chrome was configured to accept the mitmproxy root certificate for SSL/TLS interception.

Network traffic logs were captured for each session and stored securely for further analysis. Screenshots were made during every step in the testing process and a log of the steps were made.

1.2 Qualtrics Accounts

Username	First Name	Last Name	Email Address	User Type	Division	Division Admin	Actor
julian.rill+janvandermeer@surf.nl	Jan	van der Meer	julian.rill+janvandermeer@surf.nl	Standard - Qualtrics	Tech Research	Yes	Division Admin
julian.rill+johannasmit@surf.nl	Johanna	Smit	julian.rill+johannasmit@surf.nl	Standard - Qualtrics	Tech Research	No	Researcher (A)
julian.rill+pieterdejong@surf.nl	Pieter	de Jong	julian.rill+pieterdejong@surf.nl	Standard - Qualtrics	Tech Research	No	Researcher (B)

julian.rill@surf.nl	Julian	Rill	julian.rill@surf.nl	Brand Administrator	N/A	N/A	Brand Admin
julian.rill+samhoogland@surf.nl	Sam	Hoogland	julian.rill+samhoogland@surf.nl	Standard - Qualtrics	Legal Research	Yes	Researcher (C)
N/A	N/A	N/A	N/A	N/A	N/A	N/A	Anonymous Participant
N/A	Sander	Noord	julian.rill+sandernoord@surf.nl	N/A	N/A	N/A	Participant (A)
N/A	Bo	van Doorn	julian.rill+bovandoornd@surf.nl	N/A	N/A	N/A	Participant (B)

Table 14 Accounts used during technical testing within Qualtrics

1.3 Scenario 1: Login and Authentication

Business Processes

This scenario involves business processes related to **Identiteitenbeheer (Identity Management)**, which focuses on managing and making available user data and their authorisations. It also relates to **Informatiebeveiliging (Information Security)**, which ensures the continuity of information and information provision and limits the consequences of security incidents.

Features Tested

The features tested include **Multi-Factor Authentication (MFA)**, **user login with email and password**, and the option to **“Remember this device for 30 days”**. Qualtrics supports various authentication methods, including Native login and Single Sign-On (SSO), with MFA feasible for both.

Actors

- Researcher (A)

Scenario Description

A researcher attempts to log into the Qualtrics platform, providing their email address and password, and completing a two-factor authentication step, with the option to remember their device for future logins.

Prerequisites

- The Brand Administrator created an account for Researcher (A).

Steps

1. Researcher (A): Navigates to the login page.
2. Researcher (A): Enters their email address and password, and clicks 'Log In'.
3. Researcher (A): Enters their 2FA code, ticks 'Remember this device for 30 days', and clicks 'Log In'.

1.4 Scenario 2: Creating Qualtrics Projects

Business Processes

This scenario is primarily associated with **Onderzoeksplanning (Research Planning)**, which involves setting up a proposal for a study and submitting it for approval. It also broadly relates to **Applicatie-ontwikkeling (Application Development)**, as it involves developing application programs and data collections.

Features Tested

The features tested are the ability to **“Create a new project”**, specifically selecting the **“Survey” project type**, and the general process of **“Create project”**. Qualtrics allows users to start projects from scratch, enabling them to build their own questionnaires.

Actors

- Researcher (A)

Scenario Description

A researcher initiates the process of creating a new survey project within Qualtrics, navigating through the project creation interface to select the survey type and provide a name for their new project.

Prerequisites

- Scenario 1 was executed.

Steps

1. Researcher (A): Clicks ‘Create a new project’.
2. Researcher (A): Clicks ‘Survey’.
3. Researcher (A): Clicks ‘Get started’.
4. Researcher (A): Writes ‘Tech Survey’ and clicks ‘Create project’.

1.5 Scenario 3: Designing Surveys

Business Processes

This scenario is central to **Onderzoeksuitvoering (Research Execution)**, which involves the careful, verifiable, and systematic study of a specific issue to answer research questions. It also ties into **Gegevensbeheer (Data Management)**, which is about managing and making available data, and **Informatiebeveiliging (Information Security)** for sensitive data checks. Furthermore, **Kwaliteitszorg Onderzoek (Research Quality Assurance)** is relevant due to the use of ExpertReview to evaluate survey quality.

Features Tested

A wide range of question types and survey functionalities are tested, including **basic multiple-choice questions**, **Meta Info questions** (which collect background data like browser and operating system), **Signature questions**, **File upload questions**, **Text box questions** (specifically for sensitive data like bsn), **CAPTCHA questions**, and **Video response questions** with a **recording time limit**. The scenario also tests the **“Publish”** functionality and the **ExpertReview tool**, including its ability to flag **Sensitive Data Requests** and provide recommendations for survey improvement.

Actors

- Researcher (A)

Scenario Description

A researcher constructs a survey by adding various question types, such as multiple-choice, meta info, signature, file upload, and open text fields for sensitive data like a bsn, along with Captcha and video response options. They also utilise the ExpertReview feature to check for potential issues and sensitive data requests before publishing the survey.

Prerequisites

- Scenario 2 was executed.

Steps

1. Researcher (A): In the default question block, they enter 'First question', and answers 'Answer 1', 'Answer 2' and 'Answer 3'.
2. Researcher (A): Clicks 'Add new question' and selects 'Meta Info'.
3. Researcher (A): Clicks 'Add new question' and selects 'Signature'.
4. Researcher (A): Enters 'Your signature please' in the text box.
5. Researcher (A): Clicks 'Add new question' and selects 'File upload'.
6. Researcher (A): Enters 'Need a file' in the text box.
7. Researcher (A): Clicks 'Add new question' and selects 'Text box'.
8. Researcher (A): Enters 'Your bsn please' in the text box.
9. Researcher (A): Clicks 'Add block'.
10. Researcher (A): In the new text box, clicks 'Add new question' and selects 'Captcha'.
11. Researcher (A): Enters 'Just a check' in the text box.
12. Researcher (A): Clicks 'Add new question' and selects 'Video response'.
13. Researcher (A): Enters 'A nice video' in the text box.
14. Researcher (A): Ticks 'Recording time limit'.
15. Researcher (A): Clicks 'Publish'.

16. Researcher (A): Clicks 'View recommendations' under 'ExpertReview'.
17. Researcher (A): Closes the ExpertReview tab.
18. Researcher (A): Clicks 'Publish' again, enters 'My tech survey' as description, and clicks 'Publish' in the new window.
19. Researcher (A): Clicks 'Okay'.

1.6 Scenario 4: Configuring Survey Options

Business Processes

This scenario is primarily related to **Informatiebeveiliging (Information Security)**, which involves safeguarding information and information provision. It also pertains to **Gegevensbeheer (Data Management)**, as it defines how survey responses are handled, and **Performancemanagement (Performance Management)**, ensuring the organisation's functioning aligns with set objectives.

Features Tested

The features tested include accessing **"Survey options"**, configuring **"Responses"** settings such as the time limit for incomplete responses, and enabling **"Security"** features like **preventing multiple submissions**, **bot detection**, and the **security scan monitor**. Additionally, the **"Scoring"** functionality is briefly accessed.

Actors

- Researcher (A)

Scenario Description

A researcher configures the operational settings of their survey, including its name and description, defining the timeout period for incomplete responses, and activating security measures such as preventing multiple submissions, detecting bots, and monitoring for security scans.

Prerequisites

- Scenario 3 was executed.

Steps

1. Researcher (A): Clicks 'Survey options'.
2. Researcher (A): Enters 'The technical survey' as name and 'It's a simple survey really.' as description.
3. Researcher (A): Clicks 'Responses'.
4. Researcher (A): Under 'How much time should pass before they're considered incomplete?', they select '1 Hour'.
5. Researcher (A): Clicks 'Security'.
6. Researcher (A): Selects 'In Survey: prevent multiple submissions'.
7. Researcher (A): Selects 'Bot detection'.
8. Researcher (A): Selects 'Security scan monitor'.
9. Researcher (A): Clicks 'Scoring'.
10. Researcher (A): Clicks 'Back to survey builder'.

1.7 Scenario 5: Distributing Surveys to Participants

Business Processes

This scenario aligns with **Communicatiemanagement (Communication Management)**, which ensures the organisation communicates appropriately with internal and external parties. If the distribution targets potential external participants, it also relates to **Marktbewerking (Market Cultivation)**, which involves specific actions and campaigns to reach target groups.

Features Tested

The core features tested are the **email distribution** method and various **social media distribution** options, including LinkedIn, Facebook, and Twitter. Qualtrics allows users to send out questionnaires via email using either Qualtrics' mail servers or their own, and provides options for social media sharing.

Actors

- Researcher (A)

Scenario Description

A researcher distributes their survey to participants through multiple channels, specifically sending it via email and sharing it on various social media platforms like LinkedIn, Facebook, and Twitter.

Prerequisites

- Scenario 4 was executed.

Steps

1. Researcher (A): Clicks 'Distributions'.
2. Researcher (A): Clicks 'Distribute survey'.
3. Researcher (A): Clicks 'Generate a traceable link for each contact'.
4. Researcher (A): Selects 'Lists' and then 'New Contact List'.
5. Researcher (A): Enters the following contact information:
6. Email: julian.rill+sandernoord@surf.nl, julian.rill+bovandoorn@surf.nl
7. First Name: Sander, Bo
8. Last Name: Noord, van Doorn
9. Researcher (A): Clicks 'Create'.
10. Researcher (A): Clicks 'Generate Links'. This will download a .csv file with the links.
11. Researcher (A): Clicks 'Anonymous link'.
12. Researcher (A): Clicks 'Copy survey link.' This resulted in:
https://surftest.qualtrics.com/jfe/form/SV_3yljFElimPrABSK
13. Researcher (A): Clicks 'Social media'.
14. Researcher (A): Clicks 'LinkedIn'.
15. Researcher (A): Clicks 'Facebook'.
16. Researcher (A): Clicks 'Twitter'.
17. Researcher (A): Logs out.

1.8 Scenario 6: Anonymously Answering Surveys

Business Processes

This scenario is a direct part of **Onderzoeksuitvoering (Research Execution)**, focusing on the data collection aspect of a study. It also relates to **Informatiebeveiliging (Information Security)** and **Gegevensbeheer (Data Management)** due to the emphasis on anonymous responses and the collection of potentially sensitive data.

Features Tested

The testing involves opening and interacting with an **anonymous survey link**, providing input for **signature**, **file upload**, and **text box questions** (including sensitive data like bsn). It also tests the functionality of **reCAPTCHA** and **video response recording**, while ensuring the anonymity of the participant. Qualtrics offers features for **anonymous responses** by setting minimum anonymity thresholds for data points and comments.

Actors

- Anonymous Participant

Scenario Description

An anonymous participant accesses a survey via a public link and provides responses, including a signature, file upload, text input with sensitive data, and a video response, while also completing a reCAPTCHA challenge.

Prerequisites

- Scenario 5 was executed.

Steps

1. Anonymous Participant: Opens the anonymous link.
2. Anonymous Participant: Selects Answer 1, enters a random signature and uploads the file Sample Document - SURF.pdf.
3. Anonymous Participant: Closes the tab of the questionnaire.
4. Anonymous Participant: Reopens the anonymous link.
5. Anonymous Participant: Re-enters the previously mentioned data, in addition with the bsn 123456782.
6. Anonymous Participant: Clicks the '->' button.
7. Anonymous Participant: Closes the tab of the questionnaire.
8. Anonymous Participant: Reopens the anonymous link.
9. Anonymous Participant: Checks the reCAPTCHA.
10. Anonymous Participant: Clicks 'Record video'.
11. Anonymous Participant: Clicks the '->' button.

1.9 Scenario 7: Survey Answering via Targeted Links

Business Processes

Like anonymous response, this is part of **Onderzoeksuitvoering (Research Execution)** and **Gegevensverwerking en -analyse (Data Processing and Analysis)**. Given the use of personalized links, it also touches upon **Identiteitenbeheer (Identity Management)**, as it implies managing user accounts and authorisations.

Features Tested

The scenario tests interaction with a **personalized survey link**. The response process involves providing input for various question types, including **multiple-choice**, **signature**, **file upload**, **text box** (specifically for bsn), **reCAPTCHA**, and **video recording**. This tests how Qualtrics handles individual participant data collection when a traceable link is used.

Actors

- Participant (A)
- Participant (B)

Scenario Description

Two distinct participants access and complete a survey using their unique, personalized links, providing various forms of input including sensitive data, demonstrating the system's behavior for targeted survey collection.

Prerequisites

- Scenario 5 was executed.

Steps

1. Participant (A): Opens their personalised link.
2. Participant (A): Selects Answer 2, enters a random signature and uploads the file 'Sample Document - SURF.pdf'.
3. Participant (A): Reopens the anonymous link.
4. Participant (A): Enters the bsn 123456782.
5. Participant (A): Clicks the '->' button.
6. Participant (A): Checks the reCAPTCHA.
7. Participant (A): Clicks 'Record video'.
8. Participant (A): Clicks the '->' button.

After completing steps 1 until 8, repeat the exact same steps for actor Participant (B).

1.10 Scenario 8: Data Analysis on Survey Results

Business Processes

This scenario is deeply embedded in **Gegevensverwerking en -analyse (Data Processing and Analysis)**, which covers extracting, converting, cleaning, ordering, analysing, and interpreting collected research data. It also relates to **Kwaliteitszorg Onderzoek (Research Quality Assurance)** for evaluating research against quality criteria, and **Informatiemanagement (Information Management)** for reporting information to stakeholders.

Features Tested

The analysis features tested include viewing **“Results”**, utilising the **“Data Analysis”** module, examining **“Response Quality”** to identify issues like gibberish or non-descriptive text, performing **Text iQ analysis** for text interpretation, and conducting **Stats iQ analysis**, which includes **Crosstabs iQ** and **Weighting** for statistical insights. Additionally, the ability to review **“Audio & video”** responses is tested.

Actors

- Researcher (A)

Scenario Description

A researcher performs comprehensive data analysis on survey results, specifically reviewing video responses, evaluating response quality, and conducting text analysis using Text iQ. They then apply statistical methods with Stats iQ, including crosstabs and weighting, to gain deeper insights from the collected data.

Prerequisites

- Scenarios 6 and 7 were executed.

Steps

1. Researcher (A): Logs in.
2. Researcher (A): Under 'Active surveys', clicks 'Results'.
3. Researcher (A): Clicks one of the videos under 'A nice video'.
4. Researcher (A): Clicks 'Data Analysis'.
5. Researcher (A): Clicks 'Response Quality'.
6. Researcher (A): Clicks 'Text iQ'.
7. Researcher (A): Clicks 'Your bsn please' and then 'Finish'.
8. Researcher (A): Clicks 'Update'.
9. Researcher (A): Clicks 'Stats iQ'.
10. Researcher (A): Clicks 'Crosstabs iQ'.
11. Researcher (A): Clicks 'Weighting'.
12. Researcher (A): Clicks 'Audio & video'.

Appendix 2 User Type Role Permissions

1.11 General

Permission	Brand Administrator	Standard - Qualtrics
Project Permissions		
Brand Experience	On	On
Customer Experience	On	On
Employee Experience	On	On
Product Experience	On	On
Core XM	On	On
Account Permissions		
Access Mailer	On	On
Access API	On	Off
Access Organisation Address Book	On	On
Collaborate Projects	On	On
Allow JavaScript	On	On
Allow All HTML Markup	On	On
Translate Surveys with Google Translate	On	On
Download Survey Reports	On	On
Enable Public Reports	On	On
Healthcare Solutions – CX Public	Off	Off
Healthcare Solutions – CX Private	Off	Off
Healthcare Solutions – EX Public	Off	Off

Healthcare Solutions – EX Private	Off	Off
Manage Location Data	On	On
Access TotalXM Reporting Project	On	Off
Card Sorting Solution	On	On
Index Content to Research Hub	On	On
Use Alternative Method To Purchase Online Samples	Off	Off
Use Qualtrics Tickets	On	On
Use CX Dashboards	On	On
Manage Journeys	On	Off
Create CX Projects	On	On
Manage Qualtrics Tickets	Off	Off
Qualtrics Tickets Admin	Off	Off
Manage CX Users	On	Off
Stats iQ – Individual User	Off	Off
Stats iQ – Individual User – Describe	Off	Off
Stats iQ – Individual User – Relate	Off	Off
Stats iQ – Individual User – Pivot Tables	Off	Off
Stats iQ – Individual User – Regression	Off	Off
Stats iQ – Individual User – Cluster	Off	Off
Stats iQ - R Integration	Off	Off

Use Crosstabs – Individual User	Off	Off
Predict iQ – Individual User	Off	Off
Use Response Weighting	On	On
Use Imported Data Projects	On	Off
Choice Based Conjoint	On	On
Create Frontline Feedback Projects	On	Off
MaxDiff	On	On
Create Brand Tracker Projects	Off	Off
Create Brand Tracker Programmes	Off	Off
Create Brand Lift Premium Projects	Off	Off
Customise Email Headers	Off	Off
Create Brand Experience Projects	Off	Off
Create BX Dashboards Project	Off	Off
Use Brand Drivers Analysis Simulator	Off	Off
View Online Sample waves and reporting	Off	Off
Purchase Online Samples	Off	Off
Purchase Online Samples Soft Launch	Off	Off
Manage Online Sample Pricing	Off	Off
Purchase Allocations for Online Samples	Off	Off

Manage Online Samples survey allocations	Off	Off
Manage Workflows Across Projects	On	On
Manage Online Samples Templates	Off	Off
Modify SES Resources	Off	Off
Access Data & Analysis - Data	On	On
Access Data & Analysis – Audio & Video	Off	Off
COVID-19 Brand Trust Pulse	On	On
COVID-19 Dynamic Call Centre Script	On	On
COVID-19 Customer Confidence Pulse	On	On
Remote Educator Pulse	On	On
Public Health: COVID-19 Pre-Screen & Routing	On	On
Healthcare Workforce Pulse	On	On
Higher Education: Remote Learning Pulse	On	On
K-12 Education: Remote Learning Pulse	On	On
Remote + On-Site Work Pulse	On	On
Return to Work Pulse	On	On
Supply Continuity Pulse	On	On
Customer Confidence Pulse	On	On
Digital Open Door	On	On
Frontline Connect	On	On

Manage Customer Care Widgets	On	On
Use QClassroom - Course Evaluations	Off	Off
New Three Sixty Reports	Off	Off
Access EX Candidate Experience Programme	On	Off
Create Idea Screening Projects	On	On
Can Change Custom Solution Access Type	On	Off
Manage Custom Solutions	On	Off
Manage Data Access Control	Off	Off
Create Concept Testing Projects	On	On
Manage Vanity Domains	On	Off
Create Audience Management Solutions	On	On
Create Conjoint Dynamic Images Solutions	On	On
Use Vaccination Status Manager Solution	On	On
Allow Widget Pinning	On	On
View New User Navigation Tour	On	On
Embedded Widgets	On	On
Embedded Dashboards	On	On
Tiered Workflows	Off	Off
Create Reputation Management Project	On	Off
Manage BX Users	Off	Off

Use Outer Loop Projects	Off	Off
Create Outer Loop Projects	Off	Off
Use Credit Union CX Solution	Off	Off
Healthcare Certified Questions	Off	Off
Magnet Programs	Off	Off
Use Customer Experience Program	On	Off
Use Search Report	Off	Off
Use BXM Report	Off	Off
Search Research Hub	Off	Off
Access Online Panel	On	On
Create Public Audio & Video Links	On	On
Access Research Hub	Off	Off
Access Research Hub Collections	Off	Off
Access Research Hub Manage Research	Off	Off
Enable SFDC App	Off	Off
Translate Surveys with Amazon Translate	On	On
Use Social Channels	Off	Off
Push to Translation Hub	Off	Off
Enable Brand Management Hub	Off	Off
Manage Voice Pipelines	Off	Off
Access EX Benchmarks	Off	Off
Edit XM Directory	Off	Off

Load data into Location Directory	Off	Off
Manage AI Coaching Recommendations	Off	Off
Account Restrictions		
Allowed IP Addresses	All	All
Library Permissions		
Use Library Surveys	On	On
Use Library Blocks	On	On
Use Library Questions	On	On
Use Library Messages	On	On
Use Library Graphics	On	On
Use Colour Groups	On	On
Use Library Files	On	On
Use Mailing Lists	On	On
Use Panel Samples	On	On
Use Library Saved Logic	On	On
Manage Library Surveys	On	On
Manage Library Blocks	On	On
Manage Library Questions	On	On
Manage Library Messages	On	On
Manage Library Graphics	On	On
Manage Library Files	On	On
Manage Mailing Lists	On	On
Manage Panel Samples	On	On
Manage Colour Groups	On	Off
Use as Reference Library	On	On

Manage Supplemental Data	On	Off
Use Supplemental Data	On	Off
Library Restrictions		
Allowed Graphics Storage (MB)	Max	Max
Survey Permissions		
Translate Surveys	On	On
View Survey Results	On	On
View Response ID	On	On
View Restricted Data	On	On
Set Survey Options	On	On
Customise Theme	On	On
Allow Theme Images	Off	Off
Use Text Analysis	On	On
View Text Analysis	On	On
Question Permissions		
Multiple Choice	On	On
Matrix Table	On	On
Open-Ended Text	On	On
Descriptive Section	On	On
Constant Sum	On	On
Slider	On	On
Rank Order	On	On
Graphic Slider	On	On
Side-by-Side	On	On
Pick, Group and Rank	On	On

Drill-Down	On	On
Hot Spot	On	On
Heat Map	On	On
Timing	On	On
Metadata	On	On
Gap Analysis	On	On
File Upload	On	On
Dynamic Matrix	Off	Off
Captcha Verification	On	On
Net Promoter Score®	On	On
Highlight Text	On	On
Signature	On	On
Autocomplete with Google Maps	On	Off
Autocomplete with Supplemental Data	On	Off
Video Response	On	On
Calendar	On	On
Jump-Start Templates		
Banking	Off	Off
K12	Off	Off
AppPermissions		
Use Dashboard Viewer App	On	Off
Manage Dashboard Viewer App	On	Off
Use Manager Assist App	On	Off
Manage Manager Assist App	On	Off

Manage Location Experience Hub App	On	Off
Use Location Experience Hub App	On	Off
Manage Contact Centre Frontline App	On	Off
Use Contact Centre Frontline App	On	Off
Use Course Evaluations	Off	Off
View XM Platform	On	On
Use Patient Experience Hub App	Off	Off
Manage Patient Experience Hub App	Off	Off
CustomerJourneyOptimizerPermissions		
Act as Journey Analyst	Off	Off
Act as Journey Designer	Off	Off
Act as Journey Publisher	Off	Off
Act as Data Analyst	Off	Off
Act as Journeys Administrator	Off	Off
AIPermissions		
Use Insight Explorer	On	Off
EX Comment Summaries	On	On
Qualtrics Assist for EX Dashboards	On	Off
Automated Audio & Video Chapters	Off	Off
Automated Audio & Video Notes	Off	Off

Automated Audio & Video Summaries	Off	Off
Review Response Generation using AI	On	Off
XMD AI Features	On	On
Allow Research Hub Summarisation	On	On
AI Assisted Text Analytics	Off	Off
Allow Research Hub Search Relevancy Explanations	Off	Off
Brands Prompting Qualtrics Hosted LLM	Off	Off
Qualtrics Assist for CX Dashboards	On	Off
Use Agent Studio	Off	Off
EX Personalised Action Recommendations	Off	Off
Enable AI Assistance in Configuring Workflows	Off	Off
Use AI Coaching Recommendations	Off	Off

1.12 Survey Platform

Permission	Brand Administrator	Standard - Qualtrics
Project Permissions		
Brand Experience Survey Project	On	On
Customer Experience Survey Project	On	On
Employee Experience Survey Project	On	On

Product Experience Survey Project	On	On
Core XM Survey Project	On	On
Survey Platform	On	On
Account Permissions		
Create Surveys	On	On
Approve Surveys	On	Off
Approve Mailings	On	Off
'Collaborate Projects' Extends Outside Organisation	On	On
Allow Non-Accessible Surveys	On	On
Use Offline Mobile App	On	Off
Access Panel Provider API	Off	Off
Salesforce Integration	On	On
Adobe Analytics Integration	Off	Off
Access Classic Printed Reports	On	On
Use SMS Distributions	On	Off
Use SMS Access Codes	On	Off
Use WhatsApp Distributions	Off	Off
Marketo Integration	On	On
Marketo V2 Integration	Off	Off
MS Dynamics Integration	On	On
Zendesk Integration	On	On
Freshdesk Integration	On	On
HubSpot Integration	On	On
ServiceNow Integration	On	On

Use Survey Director	Off	Off
Tableau Web Data Connector	On	On
Slack Integration	On	On
Disable Full Response in Workflows	Off	Off
Tango Card Integration	Off	Off
Workflow Reporting	Off	Off
Account Restrictions		
Total Allowed Surveys	Max	Max
Allowed Active Surveys	Max	Max
Allowed Responses	Max	Max
Allowed SMS Message Credits	Max	Max
Allowed WhatsApp Message Credits	Max	Max
Allowed Outgoing Emails	Max	Max
Allowed Outgoing Emails/Week	Max	Max
Library Restrictions		
Total Allowed Panels	Max	Max
Allowed Names per Panel	Max	Max
Survey Permissions		
Delete Surveys	On	On
Edit Surveys	On	On
Copy Surveys	On	On
Activate Surveys	On	On
Deactivate Surveys	On	On

Create Response Sets	On	On
Distribute Surveys	On	On
Download Survey Results	On	On
Edit Survey Responses	On	On
Copy Survey Questions	On	On
Delete Survey Questions	On	On
Edit Survey Flow	On	On
Edit Survey Questions	On	On
Use Blocks	On	On
Use Reference Blocks	On	On
Use Conjoint	On	On
Use Triggers	On	On
Use Quotas	On	On
Use Advanced Quotas	On	Off
Use Table Of Contents	On	Off
Manage Screen-outs	On	On
Allow Tallying Screened Out Responses	On	Off
Use Crosstabs	On	On
Filter Survey Results	On	On
Use Flow Control Logic	On	On
Response Clarity	On	On
Survey Restrictions		
Allowed Responses per Survey	Max	Max
Allowed Questions per Survey	Max	Max

AIPermissions		
AI Recommended Segments	On	On
Use AI Adaptive Follow-up – Advanced	On	On
Use AI Adaptive Follow-up – Basic	On	On

1.13 Employee Experience

Permission	Brand Administrator	Standard - Qualtrics
Project Permissions		
360	On	Off
Employee Engagement	On	Off
Employee Lifecycle	On	Off
Ad Hoc Employee Research	On	Off
Account Permissions		
Create Projects	On	Off
Edit Surveys	On	Off
Manage Participants	On	Off
Manage Subjects	On	Off
Manage Evaluators	On	Off
Manage Managers	On	On
Configure Reports	On	Off
Send Invites	On	Off
View Subject Reports	On	Off
Delete Projects	On	Off
Reset Projects	On	Off
Access Directories	On	Off

Can Access Participant Personal Data	On	Off
Can Access Project Data	On	Off
Access People Import Automations	On	Off
Create Ad Hoc Employee Research	On	Off
Use Ad Hoc Employee Research	On	Off
Access EX Dashboards Project	On	Off
Cross XM Analytics Project	On	Off
Access EX Team Portal	Off	Off
Access EX25 XM Solution for Healthcare	On	Off
EX25 XM Solution for K-12	On	Off
Pulse	On	Off
Access ESG XM Solution	On	Off
Drivers of Attrition	On	Off
Access Mercer Thrive Solution	Off	Off
Question Permissions		
Tree Select	On	Off

1.14 Website Feedback

Permission	Brand Administrator	Standard - Qualtrics
Account Permissions		
Access Website Feedback	On	Off
Manage Projects	On	Off
Create Project	On	Off

Access Mobile SDK	On	Off
Library Permissions		
Use Library Creatives	On	Off
Manage Library Creatives	On	Off
Use Library Intercepts	On	Off
Manage Library Intercepts	On	Off

1.15 Contacts

Permission	Brand Administrator	Standard - Qualtrics
Account Permissions		
Manage Directory Roles	On	Off
Access XM Directory	On	On
Manage Directories	On	Off
Multiple Directories	On	Off
Access XM Directory Automations	On	Off
Use Directory Data for Dashboards	On	Off
Library Permissions		
Use Mailing List Triggers	On	Off
Manage Mailing List Triggers	On	Off

Appendix 3 Mapped Endpoints

Scenario	Endpoint	Requests	Registrar	Location
Scenario 1	pendo-static-4743056171335680.storage.googleapis.com	6	Google LLC	NL
Scenario 1	content-autofill.googleapis.com	4	Google LLC	NL
Scenario 1	android.clients.google.com	1	Google LLC	NL
Scenario 1	passwordsleakcheck-pa.googleapis.com	1	Google LLC	NL
Scenario 1	sr-client-cfg.amplitude.com	3	Amazon.com, Inc.	NL
Scenario 1	accounts.qualtrics.com	1	AKAM1-RIPE-MNT	NL
Scenario 1	s.qualtrics.com	1	AKAM1-RIPE-MNT	NL
Scenario 1	www.qualtrics.com	8	AKAM1-RIPE-MNT	NL
Scenario 1	surftest.qualtrics.com	261	AKAM1-RIPE-MNT	NL
Scenario 1	siteintercept.qualtrics.com	10	Cloudflare, Inc.	US
Scenario 1	zncydxfer8jrupnsj-qwebsite.siteintercept.qualtrics.com	1	Cloudflare, Inc.	US
Scenario 1	zn0xmxq4camg7mvzh-qxm.siteintercept.qualtrics.com	2	Cloudflare, Inc.	US
Scenario 1	data.pendo.io	11	Google LLC	US
Scenario 1	cdn.pendo.io	1	Google LLC	US
Scenario 1	api2.amplitude.com	16	Amazon.com, Inc.	US
Scenario 2	pendo-static-4743056171335680.storage.googleapis.com	N/A	Google LLC	NL

Scenario 2	www.google-analytics.com	N/A	Google LLC	NL
Scenario 2	www.googletagmanager.com	N/A	Google LLC	NL
Scenario 2	sr-client-cfg.amplitude.com	N/A	Amazon.com, Inc.	NL
Scenario 2	sr-client-cfg.amplitude.com	N/A	Amazon.com, Inc.	NL
Scenario 2	www.xm-apps-static.com	N/A	Akamai Technologies, Inc.	NL
Scenario 2	surftest.qualtrics.com	N/A	AKAM1-RIPE-MNT	NL
Scenario 2	siteintercept.qualtrics.com	N/A	Cloudflare, Inc.	US
Scenario 2	zn0xmxq4camg7mvzh-qxm.siteintercept.qualtrics.com	N/A	Cloudflare, Inc.	US
Scenario 2	zn0xmxq4camg7mvzh-qxm.siteintercept.qualtrics.com	N/A	Cloudflare, Inc.	US
Scenario 2	region1.google-analytics.com	N/A	Google LLC	US
Scenario 2	data.pendo.io	N/A	Google LLC	US
Scenario 2	cdn.pendo.io	N/A	Google LLC	US
Scenario 2	api.amplitude.com	N/A	Amazon.com, Inc.	US
Scenario 2	api2.amplitude.com	N/A	Amazon.com, Inc.	US
Scenario 2	api2.amplitude.com	N/A	Amazon.com, Inc.	US
Scenario 3	content-autofill.googleapis.com	4	Google LLC	NL
Scenario 3	surftest.qualtrics.com	255	AKAM1-RIPE-MNT	NL
Scenario 3	data.pendo.io	57	Google LLC	US

Scenario 3	api.amplitude.com	18	Amazon Technologies Inc.	US
Scenario 4	www.googletagmanager.com	1	Google LLC	NL
Scenario 4	content-autofill.googleapis.com	2	Google LLC	NL
Scenario 4	www.google-analytics.com	3	Google LLC	NL
Scenario 4	sr-client-cfg.amplitude.com	2	Amazon.com, Inc.	NL
Scenario 4	www.xm-apps-static.com	2	Akamai Technologies, Inc.	NL
Scenario 4	surftest.qualtrics.com	211	AKAM1-RIPE-MNT	NL
Scenario 4	pendo-static-4743056171335680.storage.googleapis.com	4	Google LLC	NL
Scenario 4	zn0xmxq4camg7mvzh-qxm.siteintercept.qualtrics.com	2	Cloudflare, Inc.	US
Scenario 4	siteintercept.qualtrics.com	3	Cloudflare, Inc.	US
Scenario 4	region1.google-analytics.com	2	Google LLC	US
Scenario 4	data.pendo.io	21	Google LLC	US
Scenario 4	api2.amplitude.com	2	Amazon Technologies Inc.	US
Scenario 4	cdn.pendo.io	1	Google LLC	US
Scenario 4	api.amplitude.com	12	Amazon Technologies Inc.	US
Scenario 5	www.google-analytics.com	2	Google LLC	NL
Scenario 5	content-autofill.googleapis.com	9	Google LLC	NL
Scenario 5	www.googletagmanager.com	1	Google LLC	NL

Scenario 5	pendo-static-4743056171335680.storage.googleapis.com	2	Google LLC	NL
Scenario 5	platform.twitter.com	2	Fastly, Inc.	NL
Scenario 5	abs.twimg.com	204	Fastly, Inc.	NL
Scenario 5	sr-client-cfg.amplitude.com	3	Amazon.com, Inc.	NL
Scenario 5	surftest.qualtrics.com	670	AKAM1-RIPE-MNT	NL
Scenario 5	facebook.com	2	meta-mnt, Meta Platforms Ireland Limited, RIPE-NCC-LEGACY-MNT	NL
Scenario 5	www.facebook.com	4	meta-mnt, Meta Platforms Ireland Limited, RIPE-NCC-LEGACY-MNT	NL
Scenario 5	static.xx.fbcdn.net	19	meta-mnt, Meta Platforms Ireland Limited, RIPE-NCC-LEGACY-MNT	NL
Scenario 5	zn0xmxq4camg7mvzh-qxm.siteintercept.qualtrics.com	3	Cloudflare, Inc.	US
Scenario 5	siteintercept.qualtrics.com	4	Cloudflare, Inc.	US
Scenario 5	abs-0.twimg.com	1	Twitter Inc.	US
Scenario 5	static.licdn.com	12	Fastly, Inc.	US

Scenario 5	twitter.com	1	Cloudflare, Inc.	US
Scenario 5	api.x.com	15	Cloudflare, Inc.	US
Scenario 5	www.linkedin.com	19	Cloudflare, Inc.	US
Scenario 5	platform.linkedin.com	1	Cloudflare, Inc.	US
Scenario 5	syndication.twitter.com	1	Cloudflare, Inc.	US
Scenario 5	x.com	2	Cloudflare, Inc.	US
Scenario 5	region1.google-analytics.com	2	Google LLC	US
Scenario 5	data.pendo.io	24	Google LLC	US
Scenario 5	api2.amplitude.com	9	Amazon Technologies Inc.	US
Scenario 5	cdn.pendo.io	1	Google LLC	US
Scenario 5	api2.amplitude.com	2	Amazon Technologies Inc.	US
Scenario 6	update.googleapis.com	1	Google LLC	NL
Scenario 6	clientservices.googleapis.com	1	Google LLC	NL
Scenario 6	translate.googleapis.com	1	Google LLC	NL
Scenario 6	tools.google.com	1	Google LLC	NL
Scenario 6	optimizationguide-pa.googleapis.com	1	Google LLC	NL
Scenario 6	content-autofill.googleapis.com	2	Google LLC	NL
Scenario 6	apis.google.com	1	Google LLC	NL
Scenario 6	sr-client-cfg.amplitude.com	1	Amazon.com, Inc.	NL

Scenario 6	use.typekit.net	1	AKAM1-RIPE-MNT	NL
Scenario 6	s.qualtrics.com	1	AKAM1-RIPE-MNT	NL
Scenario 6	www.qualtrics.com	6	AKAM1-RIPE-MNT	NL
Scenario 6	surftest.qualtrics.com	86	AKAM1-RIPE-MNT	NL
Scenario 6	ogads-pa.clients6.google.com	6	Google LLC	NL
Scenario 6	android.clients.google.com	1	Google LLC	NL
Scenario 6	siteintercept.qualtrics.com	1	Cloudflare, Inc.	US
Scenario 6	zncydxfer8jrupnsj-qwebsite.siteintercept.qualtrics.com	1	Cloudflare, Inc.	US
Scenario 6	client-registry.mutinycdn.com	1	Fastly, Inc.	US
Scenario 6	data.pendo.io	2	Google LLC	US
Scenario 6	api2.amplitude.com	2	Amazon Technologies Inc.	US
Scenario 7	content-autofill.googleapis.com	2	Google LLC	NL
Scenario 7	tools.google.com	1	Google LLC	NL
Scenario 7	content-autofill.googleapis.com	2	Google LLC	NL
Scenario 7	apis.google.com	2	Google LLC	NL
Scenario 7	surftest.qualtrics.com	61	AKAM1-RIPE-MNT	NL
Scenario 7	ogads-pa.clients6.google.com	5	Google LLC	NL
Scenario 8	update.googleapis.com	3	Google LLC	NL
Scenario 8	content-autofill.googleapis.com	6	Google LLC	NL
Scenario 8	www.google-analytics.com	2	Google LLC	NL
Scenario 8	csp.withgoogle.com	1	Google LLC	NL

Scenario 8	tools.google.com	1	Google LLC	NL
Scenario 8	pendo-static-4743056171335680.storage.googleapis.com	10	Google LLC	NL
Scenario 8	clientservices.googleapis.com	8	Google LLC	NL
Scenario 8	www.googletagmanager.com	1	Google LLC	NL
Scenario 8	content-autofill.googleapis.com	1	Google LLC	NL
Scenario 8	passwordsleakcheck-pa.googleapis.com	2	Google LLC	NL
Scenario 8	sr-client-cfg.amplitude.com	2	Amazon.com, Inc.	NL
Scenario 8	sr-client-cfg.amplitude.com	3	Amazon.com, Inc.	NL
Scenario 8	sr-client-cfg.amplitude.com	7	Amazon.com, Inc.	NL
Scenario 8	www.xm-apps-static.com	4	Akamai Technologies, Inc.	NL
Scenario 8	use.typekit.net	2	AKAM1-RIPE-MNT	NL
Scenario 8	p.typekit.net	1	AKAM1-RIPE-MNT	NL
Scenario 8	accounts.qualtrics.com	2	AKAM1-RIPE-MNT	NL
Scenario 8	s.qualtrics.com	2	AKAM1-RIPE-MNT	NL
Scenario 8	www.qualtrics.com	9	AKAM1-RIPE-MNT	NL
Scenario 8	static-assets.qualtrics.com	27	AKAM1-RIPE-MNT	NL
Scenario 8	surftest.qualtrics.com	3378	AKAM1-RIPE-MNT	NL
Scenario 8	content-autofill.googleapis.com	1	Google LLC	NL

Scenario 8	pendo-static-4743056171335680.storage.googleapis.com	5	Google LLC	NL
Scenario 8	api2.amplitude.com	17	Amazon.com, Inc.	US
Scenario 8	zncydxfer8jrupnsj-qwebsite.siteintercept.qualtrics.com	1	Cloudflare, Inc.	US
Scenario 8	zn0xmxq4camg7mvzh-qxm.siteintercept.qualtrics.com	11	Cloudflare, Inc.	US
Scenario 8	siteintercept.qualtrics.com	21	Cloudflare, Inc.	US
Scenario 8	zncydxfer8jrupnsj-qwebsite.siteintercept.qualtrics.com	1	Cloudflare, Inc.	US
Scenario 8	siteintercept.qualtrics.com	3	Cloudflare, Inc.	US
Scenario 8	zn0xmxq4camg7mvzh-qxm.siteintercept.qualtrics.com	6	Cloudflare, Inc.	US
Scenario 8	cdn.jsdelivr.net	1	Fastly, Inc.	US
Scenario 8	client-registry.mutinycdn.com	4	Fastly, Inc.	US
Scenario 8	client-registry.mutinycdn.com	1	Fastly, Inc.	US
Scenario 8	region1.google-analytics.com	1	Google LLC	US
Scenario 8	edgedl.me.gvt1.com	2	Google LLC	US
Scenario 8	data.pendo.io	69	Google LLC	US
Scenario 8	api2.amplitude.com	26	Amazon Technologies Inc.	US
Scenario 8	cdn.pendo.io	5	Google LLC	US
Scenario 8	api.amplitude.com	5	Amazon Technologies Inc.	US