Privacy Notice and Data processing agreement – Scottish Treasure Trove Review Public Consultation

This Annex shall be completed by the Controller, who may take account of the view of the Processor. However, the final decision as to the content of this Annex shall be with the Customer at its absolute discretion.

Robert Sandeman
Data Protection Officer
King's and Lord Treasurer's Remembrancer
Scottish Government Building
1F-North, Victoria Quay
Edinburgh
EH6 6QQ

The contact details for KLTR's Data Protection Officer are:
robert.sandeman@kltr.gov.uk

The contact details of the Supplier's Data Protection Officer are:
privacy@qualtrics.com

The Processor shall comply with any further written instructions with respect to Processing by the Controller.

Any such further instructions shall be incorporated into this Annex.

CONTROLLER

Identity of Controller for each Category of Personal Data is KLTR.

The Customer is Controller (KLTR), and the Supplier is Processor (Qualtrics)

The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Supplier is the Processor of the Data.

The Treasure Trove Review is conducting a public consultation on the Scottish Treasure Trove System. KLTR has appointed Qualtrics LLP to deliver the public consultation as a webform survey to ensure accessible distribution. Under the terms of this contract, KLTR is the data controller and Qualtrics LLP is the data processor.

Survey data

- This includes any responses given to attitudinal questions; open-ended; demographic questions (including name, email, local authority, but not age, sex, ethnicity etc.), as well as metadata about how the respondent completed the survey (such as IP addresses).
- As this is a Public Consultation we do ask survey respondents to personally identify themselves. However, respondents are able to opt out of having their responses published. Personal data may also be submitted in free text boxes. For this reason the KLTR treats survey data as personal data.

The purposes for which we process these data are:

- To help KLTR better understand the relationship the public and the heritage sector have with the Scottish Treasure Trove system, as well as to gather data on possible plans on how to improve, adapt and sustain the Scottish Treasure Trove System.

The Parties are Independent Controllers of Personal Data

The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:

- Business contact details of Supplier Personnel for which the Supplier is the Controller,
- Business contact details of any directors, officers, employees, agents, consultants and contractors of Customer (excluding the Supplier Personnel) engaged in the performance of the Customer's duties under the Contract) for which the Customer is the Controller.

Processing Duration and Retention

Controller solely determines the duration of processing. The survey will last for three (3) months. The data evaluation period is between three (3) to four (4) months.

The final report will be published by August 2024, which the data will inform. Post-report, the data will be archived and stored with KLTR (only)

for a period of twelve (12) months to inform a conclusion one (1) year later (by which point the data will then be redundant).

- As the data controller, KLTR solely determines the processing timeline, Qualtrics provides the platform.

Personal Data

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

- Personal Data is optional from the respondent. If submitted, personal data will be used to identify comments for further feedback or response from the respondent relating to the questionnaire, not for marketing purposes.
- provision of Services;
- communication to Authorized Users
- storage of Personal Data in dedicated Data Centres (multi-tenant architecture)
- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer
- execution of instructions of Customer in accordance with the Agreement.

Qualtrics shall process Personal Data within the UK only. There is no out of hours service or requirement for data to be processed or stored outwith the UK.

Storage

Data collected will be stored by KLTR in their secure digital infrastructure, delivered from their own UK-based Datacentre facilities. All KLTR data repositories are subject to specific User Access Controls and polices. Data stored in the Qualtrics platform is delivered from the supplier's UK-based Datacentre and is subject to the same User Access Controls.

Analysis

Individual level data are analysed in order to produce aggregate survey results; findings from user research and opinions are also analysed to produce aggregate results not attributed to an identifiable individual.

Dissemination

Aggregate survey results will inform the final report but will exclude personal data.

Data Collected

In terms of survey data, we process:

- Opinion data, including responses to attitudinal questions about the Scottish Treasure Trove system
- Comments data, where individuals can type their response into a free-text box and potentially disclose personal information
- Demographic data including name, email, local authority, but not age, sex, ethnicity etc.
- Metadata, including IP address

Participation in the survey is voluntary and all attitudinal, open-ended and demographic questions can be skipped.

In terms of contact information (provided optionally), we process:

- Names
- Local Authority
- Contact information (email addresses)
- Organisation and job title (if replying on behalf of an organisation)

This is collected completely separately to the survey data and provided on a voluntary basis with the consent of each individual or organisation responding. This is solely determined by the KLTR.

Data will be collected via a Qualtrics URL for Design XM. This will be posted on the KLTR website and take the Public to a webpage based questionnaire (designed by KLTR).

The software (Design XM) will collect the response from the Public and collate the information into a CSV format once the allotted time period for the consultation is over. The software will also generate an AI summative report for KLTR.

The information will be exported by KLTR in CSV format. The data can be deleted off the Cloud based license by KLTR and will be deleted by Qualtrics at the point the license expires (this is a two year license agreement).

Deletion of Data

KLTR will publish the final report in August 2024, which the data will inform. Post-report, the data will be archived and stored with KLTR (only) for a period of twelve (12) months to inform a conclusion one (1) year later (by which point the data will then be redundant).

As the data controller (KLTR), determine what Data to delete and when to delete it, Qualtrics provides the platform. KLTR will determine if it's a soft or hard delete or both within the platform. When a soft delete is performed, Data resides in production for up to 30 days before the 90-day period for removal from backups commences. When a hard delete is performed, the 90-day period for removal from backups commences immediately.

Customers requesting confirmation of Data deletion should make such request 180 days after expiry of their contract.

DISPOSAL OF MEDIA

Formal processes and procedures are in place to securely dispose of devices that may contain Customer Data. These procedures apply to all data centre environments.

Locations

Locations at which the Supplier and/or its Sub-contractors process Personal Data under this Contract.

All Data is owned and controlled by KLTR, who are designated as data controllers. Qualtrics is the data processor. KLTR and all their IT infrastructure are based in Scotland.

All data is stored in London, UK. In the event of an emergency, back-up facilities are available in Ireland. In all data centres, Qualtrics solely operates and is responsible for all system and developed software.

Protective Measures

Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect Personal Data processed under this Contract Agreement against a breach of security (insofar as that breach of security relates to data) or a Personal Data Breach.

This Schedule 2 applies to describe the applicable technical and organizational measures for the purposes of the Standard Contractual Clauses (2010), New Standard Contractual Clauses and applicable Data Protection Law.

Qualtrics will apply and maintain the Technical and Organizational Measures.

SERVICE,TECHNICAL AND ORGANISATIONAL MEASURES

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

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

Measures:

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

- Additional measures for Data Centres:
- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized

representatives have access to systems and infrastructure within the Data Center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.

- Qualtrics and all third-party Data Center providers log the names and times of authorized personnel entering Qualtrics' private areas within the Data Centers.

System Access Control

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

Measures:

- Qualtrics uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to Qualtrics' corporate network and critical infrastructure is protected by strong authentication.

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

Measures:

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

Data Input Control.

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

Measures:

- Qualtrics only allows authorized personnel to access Personal Data as required in the course of their duty.
- Qualtrics has implemented a logging system for input, modification and deletion, or blocking of Personal Data by Qualtrics or its subprocessors within the Cloud Service to the extent technically possible.

Confidentiality

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

Measures:

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

Availability Control

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

Measures:

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