GDPR information for QuenchTec Q_Panel and Q_Survey products

Introduction

Consistently with GDPR terminology our clients are referred to in this document as **Data Controller** and QuenchTec as a **Data Processor**

Data Controllers, are responsible for GDPR compliance, which mostly consists of operational procedures and documentation.

More specifically, you as our client are responsible for:

- End-user notification, consent, and withdrawal of consent
- Deciding what data, they expose to **Data Processors**
- Deciding what connections (where end user data and passwords reside) to use
- Signing up and, if necessary, creating new users
- Ensuring your users meet the age requirements and obtaining the appropriate consent if necessary (such as parental consent for children)
- Implementing the mechanisms necessary for your end users to retrieve, review, correct, or remove personal data
- Deleting user data after receiving right-to-be-forgotten requests
- Providing data in standardized formats
- Responding to your end users' privacy-related requests (DSAR)
- Responding to communications from the European Union Data Privacy Authorities
- Data breach notifications sent to supervisory authorities and end users (we will assist the customer and provide the necessary information if we are involved)
- Selecting an EU tenant when setting up your **Data Processor** tenants (us)

As a **Data Processor** QuenchTec is responsible for:

- Following the **data processor**'s instructions as explicated in a Data Processing Addendum/Agreement
- Notifying you if we receive requests from your end users exercising their GDPR rights as subjects for data access, erasure, and so on
- Notifying you if we receive requests from EU Data Privacy Authorities (unless prohibited by law enforcement)
- Notifying you if we become aware of a confirmed security breach
- Notifying you if any of our sub-processors notify us about a confirmed data breach that impacts our clients data (unless prohibited by law enforcement)
- Providing a privacy policy, terms of service, security statement, data protection agreement, and so on, to provide info on our policies and practices
- Providing information about our data processing, so that you have info it needs to process data lawfully
- Defining our services and features, how data is processed, and your rights and obligations
- Providing the means to enable you to retrieve, review, correct, or delete customer data via our solution interfaces and API's
- Providing a mechanism for you to sign up customers (panellists with consent terms and a consent agreements)

Q_Panel

If you have your own installation of Q_Panel (Marsc), you are yourself both Data Processor and Data Controller. Meaning you have to ensure that you yourself comply with all relevant GDPR rules for both. Also, please bear in mind that you will likely have local copies of much of the sensitive data

about panellists, in the form of Excel files and other files, and that it is your responsibility to handle all these in accordance with GDPR.

If QuenchTec is hosting your Q_Panel databases, we are responsible for handling the data, according to GDPR, as a Data Processor.

Data stored in Q_Panel are typically data that is covered by GDPR. E.g. a lot of personal information, like; email address, age, ZIP code, household income, marital status, number of children etc. You as a **Data Controller** is therefore tasked with making sure all this information is handled according to the GDPR rules. It is your responsibility to ensure that you are entitled to collect and store this information, through mechanisms like double opt in, and that you only use this data for the explicit uses that the panellist has consented to.

In order to assist you in complying to various GDPR rights, like the right to "get forgotten", the right "to know what information you hold" etc., we have added functions to Q_Panel. This functionality is mainly in place in version 7.04 onwards.

- A panellist can be anonymized, so that vital data for sampling can be kept, but the panellist can no longer be identified
- Any panellist data-field can be marked as anonymize-able
- Panellist profile data-fields can be marked as sensitive, which makes then hidden from all “normal” users, and only users with special privileges has access to these.
- API and user function to anonymize a panellist on request or automated
- Export functions for retrieving panellist data stored, in order to fulfil panellist right to; retrieve, review, correct, or remove personal data

Hosted databases

We are currently in the process of moving our hosed infrastructure from CityCloud, to Microsoft Azure. Both hosting providers are GDPR compliant, however there are some differences here. The databases at CityCloud, are not encrypted, the backups on the other hand are. This only has the implication of what action to take if a database should be "stolen", which is highly unlikely in both environments. If an unencrypted database is "stolen" a data breach has happened, and you/we need to inform the relevant authorities within 72 hours. If an encrypted database is "stolen" a data breach has not occurred, unless also the encryption key has been "stolen".

General comments about Q_Panel usage

Q_Panel contains information from panellists that have supplied a variety of personal and other information that is stored in a database.

In the new hosting in Azure, this database disks are encrypted and stored in the geographic area selected by you. You must therefore make sure the database is located in the appropriate area/country (legislative region), and not to mix panellist for different legislative regions into the same panel database. Thus, when collecting personal information from a panellist, the legislative region must be known. Data is also stored about what surveys they have participated in and other activity that the panellists has been involved in.

Panellists are identified by name, address, email, phone number, (ZIP code), and potentially other identifiable data like employee number. All these fields should be set as anonymize-

able variables. If a panellist requests his/her personal data to be deleted, we provide a function where these data automatically will be anonymized. Thus, the response history and profile data are kept, but it is no longer possible to correlate this data back to a particular person. It is your responsibility as **Data Controller** and owner of the panel, to identify any such fields.

As **Data Controller** you should also make sure that:

- All panellists have given consent (double opt in) and also for what purpose you will use the data
- Breach warning plan to inform authorities within 72 hours in case of data breach
- Procedure for "Right to be forgotten (anonymized)"
- Procedure for "Right to be informed by what data is stored"
- Procedure for "Portability (panellist ask to obtain a copy of the data in a for that then can be used to port to other system)

Also try to make sure that there is no link between the panellist and data stored in other systems, like answers to surveys. That way you do not need to include this data, as there is no link to this data, this data is not considered as part of the GDPR relevant data. Typically, also all survey related data is only looked at from a "aggregate" viewpoint, where it is not possible to identify responses from individuals.

Q_Survey

Platform

Currently the Q_Survey (Research Studio) platform is hosted with hosting provider CityCloud. We are also migrating this platform to Microsoft Azure, and it is our recommendation that you transition to this platform as soon as you are ready. The database at CityCloud is not encrypted, but the only difference as to GDPR compliance is that if in the very unlikely scenario that the database is "stolen", it is considered a data breach, and authorities has to be informed within 72 hours.

Type of data stored i Q_Survey

It is outside of QuenchTec control as to what kind of data that you ask in questionnaires and save in various datasets. However, as **Data Processor**, we are assuming that the data stored is considered personal data, and hence we will follow the GDPR requirements as to handling this data.

Best practices

In order to avoid having identifiable personal data stored in Q_Survey, it is advisable not to include any data that can identify the respondent as part of the data. E.g. do not store email address, or name as part of the data. In places like the UK, even a ZIP code could possibly be used to identify a person. As most common uses of survey data, is to only look at it at the aggregate level, and most surveys are conducted in an anonymised way, such data it is not considered as personal data according to GDPR.

This has the following implications:

If using a sample, try to avoid any personal data to be in the sample in the first place. You do of course need at least email or mobile number, but you should then not store this in the questionnaire (do not use the autofill function to store sample variables in the survey itself). If you need some sort of identification, in order to e.g. identify an interview for adding other data to it, in a later process, create a unique identifier for each respondent, that you store independently from the email. You may then save this identifier as part of the data, and use it to later append other data to it, where you have the same identifier, but as long as the email and identifier are stored separately, and at the moment that you "destroy" the link between them, the data collected is considered not to be personal identifiable data. You should therefore only keep the link between the two for as long as the survey requires, and then delete it as soon as possible. This also makes it possible for e.g. "one" respondent to opt out, at an earlier stage, meaning you just need to break the link.

Also, by just having the email of phone number as identifiable data in a sample, you can at any time, edit the sample and "anonymize" or delete this data. But be aware that if you have other identifiable fields in the sample, these cannot be edited. Your only option then is to delete the interview, which can influence your datasets and analysis and reports that you already have created.

In the current Research Studio hosted at CityCloud, it is possible to append sample data to respondent data, and in that way create a dataset where personal data can be identified. However, you can prevent this in two ways:

1) First remove identifiable data (edit the email column or phone number column), before you add the sample data.
2) As part of the same workflow that adds the sample data, add a tool that removes any personal identifiable data, before saving the dataset.

In the new Q_Survey platform in Azure, it is no longer possible to add sample data to respondent data directly. You have to establish a "key" that you can use to later add sample data that you have not filled into the questionnaire. You can e.g. use the respondent_ID (GUID), or the recommended separate identifier that you should allocated to such sample. In the Azure environment it is therefore by default, not possible to identify respondent data as personal data, unless you on purpose have collected such data in the questionnaire.

If you get consent to capture personal data in a questionnaire, like if it is a profiling questionnaire for a panel, or an employee survey asking for personal information, you have to make sure you follow all GDPR requirements. E.g. explicitly ask for consent and state what you are going to use the data for. If a profiling survey is conducted in the new Azure platform, it is automatically deleted after it is transferred to the target system (Q_Panel). If you collect this information in ad hoc surveys, you need to be able to delete the data if the respondent wishes so. This means you have to keep the records yourself to what surveys they have answered. You can use the "altid" as a mechanism to locate such interviews. Through the API calls it is then possible to locate specific "altid's". Once located, you have to

delete the interview, and recreate any dataset that includes this respondent's data. E.g. reload the "live" dataset, re-run any tools that you have used to create derived datasets. Also, possibly all exported data that you have created. Since this will be a time-consuming task, you should carefully consider how to conduct any such data collection where you collect personal information.

See also:
Esomar:
https://www.esomar.org/what-we-do/code-guidelines/esomar-data-protection-checklist
MRS:
https://www.mrs.org.uk/standards/gdprsupport

Client communication/Help system

We want all support and other information requests to go through our help system, "support@quenchtec.com". This ensures that communication is secure, tracked and kept for any audit or other purpose. You should avoid sending any documents or files containing any personal information, directly to any employee of QuenchTec. If such data is received, employees are instructed to delete such data immediately.

Appendix

QuenchTec Personnel

All QuenchTec personnel has singed "non-disclosure" agreements, meaning they have full understanding of how to handle client data.
All QuenchTec personnel has also received information and training in how to make sure they handle relevant aspects of GDPR in the proper way, like:

- Do not store client data on personal computers but direct all such data to our help system and protected data stores.
- Immediately delete any personal data sent to them in mail.
- Forward all support requests regarding these (and other) matters to our help system, and not answer then from their email.

QunechTec's data suppliers

We have reviews all our data suppliers to make sure they also are GDPR compliant:

Microsoft Azure (cloud hosting provider) see:
https://www.microsoft.com/en-us/TrustCenter/CloudServices/Azure/GDPR

CityCloud (cloud hosting provider) see:
https://www.citycloud.se

SendGrid (used for sending mail) see:
https://sendgrid.com/policies/tos/

Nexmo (used for sending SMS) see:
https://www.nexmo.com/blog/2017/12/14/gdpr-compliance-nexmo/

PaperTrail (used for storing WEB logs) see:
https://blog.papertrail.io/questions-about-gdpr/#.WuHiHy_JKYV

Definitions:

Data Controllers and Processors
Controller vs. Processor
Article 4 defines data controllers and data processors as below:
(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
For example, if Acme Co. sells widgets to consumers and uses Email Automation Co. to email consumers on their behalf and track their engagement activity, then with regard to such email activity data, Acme Co. is the data controller, and Email Automation Co. is the data processor.
This distinction is important for compliance. Generally speaking, the GDPR treats the data controller as the principal party for responsibilities such as collecting consent, managing consent-revoking, enabling right to access, etc. A data subject who wishes to revoke consent for his or her personal data therefore will contact the data controller to initiate the request, even if such data lives on servers belonging to the data processor. The data controller, upon receiving this request, would then proceed to request the data processor remove the revoked data from their servers.
New requirements for data processors under the GDPR
The GDPR introduces direct obligations for data processors for the first time, whereas the current Directive only holds data controllers liable for data protection noncompliance. Processors will also now be subject to penalties and civil claims by data subjects for the first time.
For starters, Article 28(1) states that:
Where 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.
In other words, data controllers, i.e. customers of data processors, shall only choose processors that comply with the GDPR, or risk penalties themselves. As supervisory authorities enforce penalties on controllers for a lack of proper vetting, processors may find themselves obligated to obtain independent compliance certifications to reassure their would be customers.
In addition, all processors are required to:

- Only process personal data on instructions from the controller, and inform the controller if it believes said instruction infringes on the GDPR (28.3). In other words, a data processor may not opportunistically use or mine personal data it is entrusted with for purposes not outlined by the data controller.
- Obtain written permission from the controller before engaging a subcontractor (28.2), and assume full liability for failures of subcontractors to meet the GDPR (28.4)
- Upon request, delete or return all personal data to the controller at the end of service contract (28.3.g)

- Enable and contribute to compliance audits conducted by the controller or a representative of the controller (28.3.h)
- Take reasonable steps to secure data, such as encryption and pseudonymization, stability and uptime, backup and disaster recovery, and regular security testing (32.1)
- Notify data controllers without undue delay upon learning of data breaches (33.2)
- Restrict personal data transfer to a third country only if legal safeguards are obtained (46)

A processor is further required to maintain a record of data processing activities if it qualifies for **any** of the following criteria (30):

- Employs 250 or more persons
- Processes data that is "likely to result in a risk to the rights and freedoms of data subjects"
- Processes data more than occasionally
- Processes special categories of data as outlined in Article 9(1)
- Processes data relating to criminal convictions

And a processor must appoint a DPO in select circumstances. Learn more here.

These new requirements will likely spawn closer coordination between data controllers and processors to ensure GDPR compliance. Existing contracts will need to be reviewed to ensure compliance, for instance clarity on the specified data processing that controllers instruct processors to perform.