Policy Owner: SecOps

Last Revision Date: May 2019

Policy Owner's Org: Quzara

Next Review Date:

Quzara Privacy Policy

Quzara Confidential

Approvals

_____ _____

Signature Date

Revision History

Date	Responsible	Summary of Change
5/08/2019	Quzara	First Release

Table of Contents

1. Introduction

This policy applies to the processing of personal data by Quzara for its clients/customers. Quzara is aware of its obligations under the relevant privacy regulations and is committed to the secure processing of personal data. This policy sets out the categories of data that Quzara stores and processes. It also sets the purposes of the processing of personal data, the legitimate basis for processing, retention of data, and data security measures implemented for personal data protection. This policy also covers Quzara's response to any data breach and data subject rights requests.

2. Definitions

Data Subject – "Data Subject" means any identified or identifiable natural person whose personal data is being collected, held or processed. Users of Quzara' services and their dependents/guests are data subjects in this context.

Personal data – "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.

Data Processing - "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, organization, structuring, storage, adaptation or alteration, retrieval,

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

3. Data Controller and Data Processor Details

Quzara acts as a data processor. In providing services Quzara processes data for client/customers. Clients/customers are data controllers who Quzara processes data for.

4. Data Protection Principles

All personal data obtained and processed by Quzara will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes of processing
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorized or unlawful processing, accidental loss, destruction or damage by using appropriate administrative, technical, and organizational measures
- comply with the relevant privacy regulation procedures for international transferring of personal data.

5. Withdrawal of Consent

Data subjects may withdraw consent at any time by filling out the Quzara Data Subject Access Request Form and submitting it to compliance@quzara.com.

6. Data Collection

Data is collected from submission of data subject's personal information by the data subject or the data subject's employer.

7. Sharing Data Subject's Data

Quzara shares data with the data subject's employer as a client/customer of Quzara services and to fulfil the contractual obligations with the data subject's employer.

Quzara may share users' personal data if it is required by applicable law, regulation, operating license or agreement, legal process or governmental request, or where the disclosure is otherwise appropriate due to safety or similar concerns. This includes sharing personal data with law enforcement officials, public health officials, other government authorities, or other third parties as necessary to enforce our data processing agreements or other policies; to protect Quzara's rights or property or the rights, safety, or property of others; or in the event of a claim or dispute relating to the use of our services.

8. Data Security

Quzara is aware of the requirement to ensure personal data is protected against accidental loss or disclosure, destruction and abuse. The security, integrity, and confidentiality of data subject's information are a priority. We have implemented technical, administrative, and physical security measures that are designed to protect against unauthorized access, disclosure, use, and modification. We regularly review our security procedures to consider appropriate new technology and methods. Quzara has implemented the following measures to assist in detecting a personal data breach:

1. Monitoring of the information system to detect:
    a. Attacks and indicators of potential attacks in accordance with unauthorized local, network, and remote connections; and
    b. Unauthorized local, network, and remote connections.
2. Identification of unauthorized use of the information system through Central Logging and Aggregation, Security Monitoring, Incident ticketing system, and Vulnerability and Configuration Scanning tools.
3. Deployment of monitoring devices:
    a. strategically within the information system to collect essential information; and
    b. at ad hoc locations within the system to track specific types of transactions of interest to the organization.
4. Protection of information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
5. Heightening of the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or governments based on law enforcement information, intelligence information, or other credible sources of information.
6. Providing automated monitoring solutions as needed; near real-time.

Actions Upon Identification of Breach

Quzara:

1. Implements an incident handling capability for personal data breach incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
2. Coordinates incident handling activities with contingency planning activities; and
3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

When Quzara is made aware of a breach, it will undertake an immediate investigation into what happened and what actions must be taken to restrict any consequences. A determination will be made at that point whether the breach is deemed a notifiable breach and whether it is deemed as resulting in a high risk to the rights and freedoms of individuals.

The controls in place for handling a personal data breach incident investigation are as follows:

1. Quzara shall evaluate the proper response to all information technology security incidents reported to Quzara.
2. Quzara shall work to decide what resources are required to best respond to and mitigate the incident.
3. After the initial reporting and/or notification, Quzara management shall review and reassess the level of impact that the personal data breach incident created.
4. An investigation into a personal data breach incident must identify its cause, if possible, and appraise its impact on systems and data. The extent of damage must be determined, and course of action planned and communicated to the appropriate parties.
5. Quzara shall coordinate incident handling activities with contingency planning activities.
6. Quzara shall investigate information system failures to determine whether the failure was caused by malicious activity or by some other means (i.e., hardware or software failure).
7. If any suspicious activities are detected, responsible personnel affected shall be notified to ensure that proper action is taken.
8. Evidence of or relating to a personal data breach shall be collected and preserved in a manner that is in accordance with privacy regulation requirements.
9. The collection process shall include a document trail, the chain of custody for items collected, and logs of all evidence-collecting activities to ensure the evidence is properly preserved for any legal actions that may ensue as a result of the incident.
10. Any system, network, or security administrator who observes an intruder on the network or system shall take appropriate action to terminate the intruder's access.
11. In the event of an active incident, management has the authority to decide whether to continue collecting evidence or to restrict physical and logical access to the system involved in the incident.
12. The Data Protection Officer will determine if other stakeholders or personnel need to become involved in resolution of the incident.
13. Quzara shall maintain records of personal data breaches and the remedies used for resolution as references for evaluating any future security breaches. The information shall be logged and maintained in such a location that it cannot be altered by others. The recorded events shall be studied and reviewed regularly as a reminder of the lessons learned. Lessons learned from incident handling activities shall be incorporated into incident response procedures, training, and testing/exercises, and implements the resulting changes.

Data Breach Notification

Quzara is fully aware of its obligations under privacy regulations in regard to data breach notification requirements to both the data subject and to relevant supervisory authorities. For full procedures and policy for data breaches please see the Data Breach Notification Policy.

9. Data Retention

In line with data protection principles, Quzara retains personal data for the duration of the service contracted for. Each contract with a client/customer is unique and duration of the service agreement will vary. Quzara will store and process data subject's personal data only for the duration agreed upon by the client/customer in providing our services. Specific contract duration will be specified in the master service agreement with each client/customer.

10. Automated Decision Making

No decision will be made about the data subject solely on the basis of automated decision making (where a decision is taken about the data subject using an electronic system without human involvement) which has a significant impact on the data subject.

11. Data Subject's Rights

Under the relevant privacy regulation data subjects have a right to receive confirmation that an organization processes their personal data, and also a right to access that data so that data subjects may be aware of it and are able to verify the lawfulness of the processing. The process for doing so is called a data subject access request and this policy sets out the procedure to be undertaken when such a request is made by the data subject regarding data processed about the data subject by Quzara.

Rights that a data subject may exercise:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object to processing
- The rights in relation to automated decision making and profiling

The right to be informed

- Providing data subjects with purposes for processing of personal data, retention periods, and who the data will be shared with
- Provided at the time of collection in the Privacy Policy Notice

The right of access

- The right to obtain confirmation that their data is being process, a copy of their personal data and other supplementary information (Privacy Policy).
- whether or not the data is processed and the reasons for the processing of the data
- the categories of personal data concerning the data subject
- where the data has been collected from if it was not collected from the data subject
- anyone who the personal data has been disclosed to or will be disclosed to, and the safeguards utilized to ensure data security
- how long the data is kept for (or how that period is decided)
- data subject's rights in relation to data rectification, erasure, restriction of and objection to processing
- data subject's right to complain to the appropriate supervisory authority if the data subject is of the opinion that their rights have been infringed
- the reasoning behind any automated decisions taken about the data subject

The right to rectification

- The right to have inaccurate personal data rectified or completed if it is incomplete

The right to erasure

- The right to have personal data erased

The right to restrict processing

- The right to limit the way that an organization uses personal data

The right to data portability

- The right to receive personal data in a machine-readable format, and the right to transmit the personal data to another controller

The right to object to processing

- Absolute right: processing data for the purposes of direct marketing
- Limited right to object in processing for:
    - Public tasks carried out in the public interest or the exercise of official authority vested in the organization
    - Legitimate interests (or those of a third party)
    - Purposes of scientific or historical research

The rights in relation to automated decision making and profiling

- Informing the data subject right of automated decision making in processing personal data (Privacy Policy)

Fees

Data Subject Requests will be provided free of charge.

If the request is manifestly unfounded, excessive or repetitive and Quzara chooses to process the request, a reasonable fee based on the administrative cost of providing the information will be charged.

Additional information needed to process a request

If additional information is needed to complete the request Quzara will contact the data subject to request the additional information necessary to fulfil the request.

Timeframe

Generally, information requested will be provided without delay and within a month.

Where requests are complex or numerous, an extension may be required. Quzara will respond to the request within a month to explain why the extension is necessary.

Refusing a request

Quzara may refuse to comply with a subject access request if it is manifestly unfounded or excessive, or if it is repetitive. In these circumstances, Quzara will inform the data subject

without undue delay and within one month of receipt with explanation why Quzara is unable to comply. The data subject will be informed of the right to complain to the appropriate supervisory authority and to a judicial remedy.

How Data Subject Requests will be received and fulfilled

Data subjects may make requests by filling out the "Quzara Data Subject Request" form and emailing it to compliance@quzara.com

12. Supervisory Authorities,

As a US-based company Quzara does not report to one specific supervisory authority, but respects and accommodates to all supervisory authority requests for relevant privacy regulations.

13. Data Protection Impact Assessments

Quzara conducts regular data protection impact assessments. These assessments include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purposes
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Full record of data protection assessments can be found in the *data protection impact assessment register*

14. Data Protection Officer

Quzara is dedicated to the principles laid out by data privacy regulations and has appointed a Data Protection Officer (DPO) to oversee all data protection and data privacy matters within Quzara. Inquiries or concerns are received by Quzara's Data Protection Officer Alexander Choi. The Data Protection Officer can be contacted at compliance@quzara.com

Responsibilities of the Data Protection Officer are the following:

- Inform and advise the company and employees how to comply with data protection regulations
- Monitor the company's compliance with the data privacy regulations, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
- Give advice and recommendations to the company about the interpretation or application of the data protection rules and regulations
- Handle complaints or requests by the relevant supervisory authorities, the data controller, data subjects, or introduce improvements on their own initiative
- Report any failure to comply with applicable data protection rules
- Monitor compliance with data protection laws
- Identify and evaluate the company's data processing activities
- Cooperate with the relevant supervisory authorities

- Act as the contact point for supervisory authorities on issues relating to personal data processing and to consult, where appropriate, with regard to any other matter
- Maintain the records of processing operations
- Report to the highest level of management at the company
  The Data Protection Officer has the authority to:

- Make decisions regarding data subject requests allowable under the relevant data protection legislation
- Represent the organization to supervisory authorities with regard to data protection issues