Privacy policy

Terms and Definitions

Term	Definition
Autoriteit Persoonsgegevens	The supervisory authority within the Netherlands regarding privacy.
Automated individual decision-making	The process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data.
Data breach	Unlawful access to, destruction, modification or release of personal data from an organization without permission of that organization due to a security incident. Examples of data breaches include (but are not limited to): Loss of a portable memory device, Theft of company laptop, Hacking/malware/phishing , Accidental publication (e-mail sent to wrong e-mail address), Calamities (fire in datacenter)
Data Subject	Identified or identifiable natural person.
General Data Protection Regulation (GDPR)	The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in European law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA) since 25th of May 2018.
Information security incident	An adverse event that poses a threat to the confidentiality, availability, and integrity of information within the organization. Examples of information security incidents are DDoS/Attrition, web attacks (drive by infections), email attacks (Phishing, SPAM, Virus infections), improper usage, loss or theft of equipment, outage, unauthorized access and data breaches.
Personal data	Means any information relating to an identified or identifiable natural person.
Processing (activities)	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.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in

	particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

1. Introduction

QuantIQ B.V. (henceforward QuantIQ) analysis personal data of customers for their clients in order to predict future customer behavior. In order to do so, QuantIQ uses automated individual decision-making, including profiling. Taking into account the nature, scope, context and purpose, QuantIQ is aware of the responsibility for what QuantIQ does with personal data and the need to comply with the principles set forth within the European data protection legislation, the GDPR (General Data Protection Regulation).

This privacy policy sets out to demonstrate compliance with the GDPR. The policy is drawn up within proportion of the processing activities done by QuantIQ.

2. Scope

The policy applies to:

- Everybody employed by QuantIQ;
- Where applicable, to external parties who work on behalf of QuantIQ or who have been given authorized access to information and information systems within QuantIQ;
- All data, programs, systems, facilities, and other technical infrastructure under the responsibility of QuantIQ.

This privacy policy makes it possible for employees to know his/her responsibility when processing personal data and to be attentive to work in accordance with the requirements of the GDPR and this privacy policy. It is required for employees to take notice of this policy and understand their roles and responsibilities regarding privacy.

3. Roles and Responsibilities

All roles and responsibilities are shared by the two directors of QuantIQ.

4. Lawfulness, fairness and transparency

QuantIQ only processes personal data fairly and in accordance with data protection legislation. The data subject will be informed about the processing activities with clear information which is easily accessible.
QuantIQ primarily processes personal data based on the following legal basses:

- The performance of a contract
    - Processing is 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.
- The legitimate interests pursued by QuantIQ

- Processing is necessary for the purposes of the legitimate interests pursued by QuantIQ or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject.

- To comply with a legal obligation
  - Processing is necessary for compliance with a legal obligation to which the entity of QuantIQ is subject.
- Data subject has given consent
  - Processing is based on the given unambiguously consent of the data subject that his/her personal data is processed for one or more specific purposes.

4.1. Requirements when data subject has given consent

When personal data is processed by QuantIQ based on the legal basis of consent, the following requirements apply:

- Personal data may only be processed if the data subject has given his/her consent to the processing.
- QuantIQ is able to demonstrate that the data subject has consented to the processing of the personal data. QuantIQ must provide the following:
  - The consent needs to be documented and retained;
  - The data subject must be informed about
    - the purposes of the processing for which consent is required;
    - which entity is responsible for the processing;
    - of the potential consequences of the processing for the data subject;
    - of the right to withdraw his/her consent at any time;
    - that withdrawal of consent does not affect the lawfulness of the relevant processing before such withdrawal.
  - When other matters are also mentioned while giving consent, the request for consent needs to be clearly distinguishable from the other matters.
  - The consent must be presented in an easily accessible form, using clear and plain language.
  - The consent needs to be withdrawn as easy as it is to give consent.
- When the data subject is an employee, consent generally should not be used as a legal basis for Processing. Employees may be asked to consent to Processing of Personal Data only if:
  - The processing has no foreseeable adverse consequences for the employee.
  - If an employee applies for employment or other work engagement with QuantIQ, QuantIQ may request the data subject's consent to process his/her personal data for purposes of evaluating his/her application.

The data subject may deny or withdraw consent at any time. Upon withdrawal of consent, QuantIQ will discontinue processing as soon as reasonably practicable. The withdrawal of consent shall not affect the lawfulness of the processing:

- Based on such consent before its withdrawal;
- Of the relevant personal data based on other legal grounds.

5. Categories of Personal Data

QuantIQ is committed to processing only the personal data which is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. It is also our responsibility to ensure that the personal data processed is accurate and kept up-to-date, with any inaccuracies being rectified or erased without delay.

5.1. Client data

In delivering our services, we may process a selection or all of the following personal data:

- Identity Data: Such as first and last name.
- Contact Data: This includes email address, physical address, and phone number.
- Behavioral Data: This encompasses lifestyle characteristics such as family composition, marital status, etc.
- Geographical Data: Four-digit postal code.
- Usage Data: Information about how customers use products and services.
- Marketing and Communications Data: This includes preferences in receiving marketing and communication preferences.

5.2. QuantIQ Platform data

In addition to the client data, QuantIQ also collects and processes data generated through the use of our software platform. This is to enhance user experience, improve our services, and for analytical purposes. This may include information like user activity, engagement data, device and browser information, and IP address.

Please note that the specific types of personal data processed will depend on the customer. While we aim to minimize the personal data we process, the nature of our services may require us to process a broad range of personal data.

5.3. Cookies

As part of QuantIQ's commitment to transparency, we use cookies on our website. These small text files improve user experience by remembering preferences and aiding site interactions.

Our use of cookies includes necessary functions, performance analysis, content personalization, and possibly advertising.

Third-party services on our website may also use cookies, over which QuantIQ has no control. We recommend reviewing their respective policies for more information.

You can manage or disable cookies in your browser settings, but this may impact your experience and the services we can provide.

6. Purpose of processing activities

QuantIQ will only process personal data 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 only be done if this is compatible with the initial purposes and, where applicable in consultation with a controller.

→ Processing of employees personal data is necessary for the following purposes:
  - Human resources and personnel management
  - Employee recruitment
  - The performance of an employment or other contract with an Employee
  - Payroll and administration of Employee benefits

→ Processing of customers personal data, provided by a controller, is necessary for the following purposes:
  - Analyzing future customer behavior
  - Performing other data analysis

→ Processing of client personal data
    - Website visitors

7. Third parties receivers of personal data

QuantIQ might share personal data with the following third parties for operational, marketing, and support purposes:

- Google Cloud Platform
- GSuite
- Microsoft Azure
- Our email communication system for sending newsletters and updates.
- Our support ticketing system for handling customer inquiries and issues.

We ensure that all third parties maintain adequate data security and privacy standards.

8. Retention period of personal data

QuantIQ's software product includes Data Analysis Services, processing and analyzing data to deliver insights. The retention periods are:

- Training Services Data: Deleted two months post completion.
- Data Analysis Services Data: Retained for three months post project completion or as per the processor agreement.
- Customer Data: Retained for the duration of our contractual relationship, then deleted or anonymized.
- Platform Usage Data: Anonymized and retained indefinitely for service improvement.
- Marketing Data: Kept until opt-out or deletion request.

Anonymized data may be kept longer. For detailed provisions, refer to our Data Retention Policy.

9. Data Subject Rights

This chapter sets out the protocol to ensure that the data subject's rights are performed accordingly. Procedures for complying with a request for a data subject' rights are outlined, whether personal data is processed by QuantIQ as a controller or as a processor..

9.1. Types of Data Subject' Rights

According to the GDPR, every data subject has the right to request:

- Access to his/her personal data
- To rectify his/her personal data
- To erasure of his/her personal data
- To restriction of processing his/her personal data
- To data portability (a transfer) of his/her personal data to another organization;
- To object his/her personal data.

9.2. Procedure (controller)

When requesting a right, a data subject should send his/her request via email to privacy@churned.nl.

Prior to fulfilling the request of the data subject, QuantIQ may require the data subject to specify:

- The circumstances in which QuantIQ obtained the personal data.

- The process and/or categories of personal data to which he/she is seeking access.
- The system in which the personal data is likely to be stored, to the extent reasonably possible.
- In case of a request for rectification, deletion, or restriction, the reasons why the personal data held by QuantIQ is incorrect or incomplete.

When a right is requested by the data subject, the data subject:

- Needs to provide proof of his/her identity. When QuantIQ has reasonable doubts concerning such identity additional information enabling his/her identification needs to be provided.
- Pay a fee to compensate QuantIQ for the reasonable costs relating to fulfilling the request provided QuantIQ can reasonably demonstrate that the request is manifestly unfounded or excessive (e.g. because of its repetitive character). Otherwise the fulfillment of the request does not need to be compensated.

9.3. Procedure (processor)

When a right is requested by the controller on behalf of the data subject, the controller should send the request via email to privacy@churned.nl.

9.4. Response Period

Within one calendar month of QuantIQ receiving the request and any information necessary mentioned, the contact person shall inform the data subject or controller in writing or electronically either

- of QuantIQ position with regard to the request and any action QuantIQ has taken or will take in response,
- the ultimate date on which he/she will be informed of QuantIQ's position and the reasons for the delay, which shall be no later than 2 calendar months after the original one month period.

9.5. Denial of Requests

QuantIQ may deny a data subject's request if:

- The request does not meet the requirements;
- The request is not sufficiently specific;
- The identity of the relevant data subject cannot be established by reasonable means, including additional information provided by the data subject.
- QuantIQ can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g., because of its repetitive character. A time interval between requests of 1 year or less shall generally be deemed to be an unreasonable time interval.

9.6. Complaint

A data subject may file a complaint or claim with the supervisory authority or the courts if:

- The response to the request is unsatisfactory to the data subject (e.g. the request is denied).
- The data subject has not received a response as required.
- The time period provided to the data subject is, in light of the relevant circumstances, unreasonably long, and the data subject has objected but has not been provided with a shorter, more reasonable time period in which he/she will receive a response.

10. Data Storage

All personal data collected by QuantIQ is stored securely within data centers located in the European Union. These data centers adhere to the highest standards of infrastructure security and data protection.

11. Information Security Incidents

This chapter sets out the protocol to ensure a consistent and effective approach to the management of information security incidents and data breaches. Procedures for reporting and managing information security incidents are outlined.

The controls outlined in this protocol apply to all locations from which information and information systems can be accessed and to all information created, managed, or received by QuantIQ in any format, stored in any system or device.

11.1. Responsibilities

All employees who have been authorized by QuantIQ and have access to networks and information systems, are responsible for immediately reporting a/an (suspected) information security incident involving information from QuantIQ.

The privacy contact person is responsible for acting as the first line, collecting and documenting relevant details as evidence, storing the evidence of an information security incident in the appropriate systems and assessing the incident in consultation with the (external) privacy lead. When necessary, communicating the existence of an information security incident to relevant controllers (in case QuantIQ is the processor) or to the supervisory authorities (in case QuantIQ is the controller).

The (external) privacy lead is responsible for acting as the second line and classifying the information security incident when necessary.

11.2. Committing information security incidents

Users who report an information security incident can do so freely. Unintentionally committing an information security incident will not result in any disciplinary measures. However intentionally causing an information security incident may result in disciplinary measures by the CEO, up to immediate dismissal.

11.3. Procedure

The following procedure will be followed when reporting a/an (suspected) information security incident.

→ The privacy contact person will assess whether a suspected information security incident is an actual incident;
→ When the privacy contact person can solve the incident, the privacy contact person will:
- Offer first line support;
- Collect, document, and register all relevant details as evidence within the appropriate system;
- Send a summary to the (external) privacy lead for information with all relevant data.
    - Status of the incident (is it resolved or not, how is it resolved etc.)
    - Other information that might be relevant

→ When the privacy contact person cannot address the actual information security incident, the privacy contact person will:
- Deploy the (external) privacy lead for second line support to manage the incident;

- Collect and document all relevant details as evidence and send it to the privacy lead for investigation.

11.4. Data breach

In case the information security incident is classified as a data breach, the following information needs to be provided:

- Date and time when the data breach was discovered;
- Data / Period when the data breach took place;
- Description of how the incident could take place;
- Nature of the incident (accessing, copying, changing, removing / destroying, etc.);
- The categories of data subjects (the subjects of the personal data, e.g. employees, customers, third parties) that can be affected by this incident;
- An estimation of how many data subjects may be affected by the data breach;
- Which categories of personal information were involved in the data breach, specify if sensitive personal information was involved in the data breach;
- If the personal information was encrypted at the time of the data breach or was otherwise made incomprehensible or inaccessible.
- If the data subjects can be negatively affected by the data breach;
- If the data breach is reported to the data subjects;
- Other information that might be relevant.

11.4.1. Reporting a data breach to the controller (processor)

If the information in a data breach entails information of clients where QuantIQ is classified as a processor, the following procedure will take place:

- The privacy contact person informs the controller of the data breach without unreasonable delay and will provide all relevant information to the controller.
- The controller will subsequently assess the incident and will determine if the incident will be reported to the supervisory authority and the affected data subject.

11.4.2. Reporting a data breach to the relevant authorities (controller)

The following information needs to be reported to the qualified authorities if QuantIQ is classified as the controller:

- Nature of the incident (accessing, copying, changing, removing / destroying, etc.);
- The categories of data subjects (the subjects of the personal data, e.g. employees, customers, third parties) that can be affected by this incident;
- The categories of data subjects (the subjects of the personal data, e.g. employees, customers, third parties) that can be affected by this incident;
- An estimation of how many data subjects may be affected by the data breach;
- Which categories of personal information were involved in the data breach, specify if sensitive personal information was involved in the data breach;
- If the personal information was encrypted at the time of the data breach or was otherwise made incomprehensible or inaccessible;
- If the data subjects can be negatively affected by the data breach;
- If the data breach is reported to the data subjects;
- The name of a contact person when further information is required;
- Other information that might be relevant.

The privacy contact person will ultimately, in consultation with the (external) privacy lead, decide whether a data breach needs to be reported to the supervisory authority.

11.4.3. Reporting a data breach to data subjects (controller)

The data protection law states that, if necessary, the data subject will be informed of the data breach if it entails their personal data. This is required when there is a high possibility that the data breach will have a negative impact on the data subject (e.g. identity fraud). When the breach entails sensitive personal data, the data subject must be informed.

The privacy contact person will ultimately, in consultation with the (external) privacy lead, decide whether a data breach needs to be reported to the data subjects.

11.4.4. Refraining from reporting a data breach

QuantIQ may delay or refrain from providing such notifications to a controller, the supervisory authority or affected data subject(s) if otherwise prohibited, such as if a law enforcement official or a supervisory authority determines that notification would impede a (criminal) investigation or cause damage to national security or the relevant industry sector. In this case, notification shall be delayed or withheld as instructed by such law enforcement official or supervisory authority

12. Technical and organizational information security measures

QuantIQ has taken the following technical and organization information security measures to avoid incidents:

- Logical access control, using passwords
- Physical measures for access security
- Automatic logging of all actions concerning personal data
- Encryption of all digital information concerning personal data
- Organizational measures for access security
- Security of network connections
- Targeted access restrictions
- Control on authorizations
- Two-step authentications on cloud providers

13. Compliance with the policy

QuantIQ ensures compliance with this privacy policy through regular reviews by the privacy contact person and mandatory policy awareness for all employees. Suspected breaches should be reported to the privacy contact person. Non-compliance may result in disciplinary action, including potential termination of employment. The policy will be periodically updated to reflect legislative, technological, or business changes