# QRIDI OY
# DATA PROTECTION RULES

*The Qridi Oy data protection rules document was updated on 4 January 2021*

## 1. BACKGROUND AND PURPOSE OF THE RULES

Qridi Oy (hereinafter 'Company') must, in its operations and the processing of personal data, adhere to the EU's General Data Protection Regulation (EU) 2016/679, the supplementary Finnish Data Protection Act (1050/2018) and the requirements laid down in these documents.

These data protection rules were prepared for the use of the Company itself as well as its clients and other interest groups to describe the data processing conducted by the Company and ensure that those who process personal data on the Company's behalf are aware of their rights and responsibilities in this regard. The purpose of the rules is to increase openness in data protection matters and ensure the lawful processing of personal data within the Company. The Company's employees and interest groups process personal data collected or held by the Company and are thereby obliged to observe the data protection rules prepared by the Company. The lawful and safe processing of personal data is an important part of the Company's operations, and it helps to secure strong and long-lasting customer relationships.

## 2. DATA PROTECTION

Data protection refers to restricting the collection and processing of personal data in order to safeguard privacy. Everyone has the right to privacy in the context of personal data processing.

The term 'personal data' refers to all information concerning a natural person. The Company is in possession of personal data on its clients, potential clients, employees and the users of the Qridi learning environment and website, which the Company's employees may have access to for the purpose of handling their work tasks. The processed personal data includes details, such as names, telephone numbers, e-mail addresses and photos. The personal data also includes other details that can be indirectly linked to an individual, such as the computer's IP address or other data stored in the Qridi learning environment, which can be used together with other available information to identify the person in question.

The data protection legislation lays down obligations related to data processing with which the controller and processors must comply. The Company conducts most of its processing activities in the role of a processor, which means the Company's clients, i.e. subscribers to the Qridi software service, are controllers as regards the personal data collected based on use of the software service. As regards its own employees, however, the Company serves as a controller. This also applies to marketing and sales activities in the context of which a client and marketing register is created for the Company. In these cases, the processing of personal data can sometimes be outsourced to a third party.

## 3. WHY IS DATA PROTECTION AN IMPORTANT PART OF QRIDI OY'S OPERATIONS?

The rules stem from the aforementioned EU's General Data Protection Regulation (hereinafter 'GDPR'), which must be applied in all EU Member States. In addition to the GDPR, Finland applies the national Data Protection Act as a supplementary general piece of legislation.

As a general rule, the GDPR covers all processing of personal data within the EU and every operator that holds a register containing information on one or more natural persons, such as clients or employees, regardless of the volume and extent of the processing or the size of the operator. Therefore, the Regulation also applies to the Company's operations and must be observed within their scope.

The Company must be able to demonstrate compliance with the GDPR. In practice, this means the continuous planning of personal data processing at the level of the organisation and its information systems, more extensive and detailed documentation management, agreement updates and personnel training with regard to personal data processing.

Adherence to the data protection legislation ensures that the Company's clients, users of the Qridi learning environment, employees and students can be sure that their personal details are protected. The legislation provides individuals with extensive rights with regard to their own personal data. One of the key rights is the right of individuals to access personal data regarding them and demand relevant information. The controller is responsible for ensuring that these rights are fulfilled. It is the obligation of the processors of personal data to help the controller meet the rights of data subjects.

For the reasons listed above, these data protection rules aim to provide a clear picture of the personal data processing conducted by the Company. The transfer of personal data to parties external to the Company as well as the processing of personal data by the Company itself requires a separate agreement with the recipient of the information.

The legislation requires the authorities to be notified of any observed data breach, such as hacking, within 72 hours. If the processing of personal data fails to meet the requirements set forth in the legislation, the violation may result in a fine. The sanction may be imposed on the controller and processor.

## 4. DATA SECURITY

Data protection is different from data security which refers to technical solutions aimed at ensuring that external parties do not gain access to personal data (this includes firewalls, data encryption systems and passwords). In other words, ensuring data protection requires functional and efficient data security solutions.

Data security means maintaining the availability, confidentiality and integrity of information. Availability means that the information is accessible when needed. Confidentiality means that the information can only be accessed by those who have the right to do so. Integrity means that the information is accurate and cannot be edited or destroyed by any external party.

Data security must be considered in every life cycle phase and process related to personal data from HR management to cooperation with interest groups. Data secure operations is one of the ways to implement data protection, and the Company has ensured appropriate data security and level of confidentiality through technical and organisational measures. The Company has prepared separate written data security practices that cover these measures.

## 5. GENERAL DATA PROTECTION PRINCIPLES

The legislation sets limits for the kinds of personal details the Company can collect and the grounds and methods for their processing. Personal data must be processed as described below.

- Personal data must be processed in a lawful, fair and transparent manner from the perspective of the data subject (*lawfulness, fairness and transparency*);
- The personal data must be collected for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes (*purpose limitation*);
- The personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (*data minimisation*);
- 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 (*accuracy*);
- The personal data must kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (*storage limitation*);
- The personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (*integrity and confidentiality*).

## 6. QRIDI OY'S OBLIGATIONS AS A PROCESSOR OF PERSONAL DATA

Insofar as the Company's processing of personal data is based on an order made by a corporate client (educational institution, municipality, club, company or similar organisation) and the Company is processing the personal details of students, athletes or parents/guardians that are stored in Qridi's software service, the Company is to be regarded as a processor, as specified in the data protection legislation.

The Company has prepared a statutory privacy policy on the processing measures conducted on behalf of each controller (corporate client) and adheres to it in the processing of personal data, alongside these data protection rules and processing agreements made with the controllers.

The Company has, in cooperation with each controller for which it processes personal data, prepared a mutual written agreement that lays down detailed provisions on the processing of the personal data. The Company processes personal data only in accordance with these agreements and the instructions provided by the controllers. The Company has ensured that it has deployed sufficient safeguards to carry out the appropriate technical and organisational measures in such a way that the processing of personal data meets the requirements of the data protection legislation in order to secure the rights of the data subjects.

The Company has ensured that all persons who operate under it and have the right to process personal data have been introduced to their duties in relation to the processing of personal data as well as these data protection rules and, if necessary, the rules provided by the controller, and that they have committed to confidentiality or are bound by the appropriate statutory obligation to confidentiality.

When acting as a processor, the Company may not employ the services of another processor without obtaining express or general written permission from the controller in advance. If the Company has agreed with the controller to outsource a portion of the data processing activities, the Company must inform the controller of all planned changes regarding the increase in number or replacement of personal data processors, so as to provide the controller with the opportunity to object to such changes.

The agreement between the Company and controller binds the Company to the controller with regard to the following matters, for example: object and duration of the processing, nature and purpose of the processing, type of personal data, groups of data subjects, and the rights and responsibilities of the controller. As a processor of personal data, the Company is bound by the following provisions set forth in Article 28 of the GDPR, such that the Company

1. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
2. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
3. takes all measures required pursuant to Article 32;
4. respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
5. taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
6. assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
7. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
8. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

Furthermore, where the Company engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract between the Company and the controller must be imposed on that other processor, and the personal data processing performed by that other processor must provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, the Company will remain fully liable to the controller for the performance of that other processor’s obligations.

## 7. QRIDI OY'S OBLIGATIONS AS A CONTROLLER

As regards the Qridi software service, the Company primarily serves its clients in the role of a processor. In these cases, the client is question is the controller. In the event of any questions with regard to how the controllers process personal data, we recommend direct contact with the controller in question (school, municipality, club, company or other organisation that uses Qridi services).

As regards the personal data of the Company's own employees, potential clients or the contact persons of existing clients, the Company serves as a controller. The GDPR defines certain essential obligations that apply to the controller.

### *7.1 Accountability*

Upon each enquiry, the controller must be able to demonstrate compliance with the provisions of the GDPR. The Company has met its accountability obligation through the following measures:

- The processing of personal data is transparent: the privacy policy or corresponding documentation is kept up to date and available to the data subjects. The Company has privacy policies that pertain to the employee register and client and marketing register, and these are available on the Company's website.

- Data security is maintained. This refers to technical systems and ensuring that each party processing personal data is aware of their relevant rights and obligations with regard to the information being processed. The data security practices prepared by the Company are observed in the Company's operations. All employees who process personal data have been introduced to the obligations related to the processing of personal data as well as these data protection rules.

- Data subjects must always be notified of the processing of their personal data or any changes thereto. The Company has informed and is informing the data subjects on the data processing upon the collection of personal data, as required by the GDPR. The data protection rules regarding the processing are also available on the Company's website.

- If personal details are disclosed to an external service provider, a separate agreement on the processing of this personal data must be prepared. In these cases, the agreement must always include the terms and conditions listed in Article 28 of the GDPR.

- If personal data falls into the wrong hands in one way or another (data breach), the supervisory authority and possibly the data subject must be informed of the matter. The Company is prepared to prepare such notification as described below.

- The registers and data files may not be used to store personal details for the processing of which there are no longer any grounds. The Company will store personal data only for as long as the processing of the data is justified. It will delete the data when the processing right ends. The Company has specified storage periods for personal data in advance and monitors adherence to them regularly.

### *7.2 Obligation to ensure a legal basis and purpose for the processing of personal data*

There must always be a basis and purpose for the processing of personal data, which means that personal details cannot be collected without a predetermined purpose.

The GDPR specifies six bases by virtue of which personal data can be lawfully processed. Four of them apply to the Company as a controller and form the legal basis for the data processing (even one basis is sufficient):

- data subject's consent,
- legitimate interest for the data processing,
- agreement based on which the data is processed, or
- legal obligation.

As regards the personal data processed by the Company, one of the bases listed above must be met for each group of data subjects, resulting in the Company having the right to process the personal data.

### *7.3 Obligation to notify of data breaches*

One of the controller's essential obligations applies to activity in the context of data breaches. As a general rule, the controller is always obliged to provide notification of such breaches, regardless of their scope.

**Notification obligation in brief**:

- As the controller, the Company must report data breaches to the supervisory authority (Office of the Data Protection Ombudsman) without undue delay immediately upon becoming aware of the incident and, where possible, within 72 hours.
- Exceptions to this are cases where the controller *can demonstrate* that the personal data breach is unlikely to cause risks related to the rights and freedoms of natural persons.
- If the notification cannot be issued within 72 hours, the controller must provide the supervisory authority with a justified statement.
- All data breaches must be documented and, where necessary, the documents must be presented to the supervisory authority.
- Information related to a data breach can be provided to the appropriate authority in phases.

**Notifying data subjects of a data breach**

In the event that a personal data breach is likely to result in a high risk to individuals, the controller must, without delay, notify the data subjects themselves of the breach, in addition to the supervisory authority.

Naturally, the notification does not need to be issued to everyone, only those affected by the data breach.

The data subjects do not need to be notified if:

- encryption or other reliable methods that achieve the same result have been used in the storage of the personal data, or
- the Company has ensured that the high risk to the data subjects' rights is *no longer likely to materialise*.

## 8. DISCLOSURE AND TRANSFER OF PERSONAL DATA

Personal data may only be disclosed and transferred in accordance with the principles listed in these data protection rules.

The Company will not disclose personal data to other controllers in its role of a personal data processor. In the role of a controller, the Company may disclose personal data to another controller if there is a legal basis for this and the recipient has the right or authorisation to receive and process reliable personal data based on the GDPR. Personal data will not be disclosed to third parties for marketing purposes.

For the purpose of its operations, the Company may transfer personal data to third-party service providers for processing in its role as a controller or personal data processor. However, in the role of a personal data processor, this is only possible if the controller's written permission has been obtained in advance. The third-party service providers serve as processors of personal data on behalf of the Company. The transfer of personal data is conducted in accordance with the requirements set forth by the data protection legislation and by virtue of the legal bases and purposes of use presented in these data protection rules. The Company has ensured that the service providers it uses adhere to the data protection legislation. Through agreement arrangements, it has also made sure that the service providers maintain a sufficient level of data protection and data security to safeguard the transferred personal data. The service providers regularly used by the Company are listed in the documentation related to data security practices.

In contexts where the Company is the personal data processor, the countries or areas where the personal details are stored are specified in the customer agreement, which means that the Company has written advance permission from the controller for any possible transfers of personal data. Where the Company is the controller, the personal data is stored in data centres located within the EEC. However, some of the service providers used by the Company may backup information to locations in the United States, outside the EU/EEC area.In these situations, the Company has ensured sufficient data protection as regards the countries in question and the appropriate protective measures for the personal data, so that the data subjects' rights and effective means of legal protection are secured.

## 9. DATA SUBJECT'S RIGHTS

The applicable legislation provides the data subjects with extensive rights in relation to their personal data. The data subjects' rights are obligations to the controller. The section below lists the rights of the data subjects which the Company must ensure in the role of the controller, i.e. in relation to client representatives, contact persons and its own employees.

### *9.1 Right to be informed of the personal data processing*

Data subjects always have the right to know whether or not the Company is processing their information. All enquiries should be addressed to info@qridi.fi. If information is processed, the relevant data subject has the right to be informed of the stored personal details and the following:

- The personal details that have been stored and the purpose of the storage.
- The recipients or recipient groups to which the Company has disclosed or intends to disclose personal data.
- Where possible, the planned storage period of the personal data or, if the storage period cannot be reported, the criteria for defining it.

### *9.2 Right to the rectification of personal data*

Data subjects have the right to demand the Company to rectify, without undue delay, any inaccurate and erroneous personal data regarding them.

### *9.3 Right to be forgotten and object to the processing of one's personal data*

Persons included in the file have the right to demand the removal of their personal data or restriction of the processing and object to the processing of their data. Where the processing is based on the data subject's consent, the data subject may withdraw the consent at any time. Data subjects have the right to prohibit the controller from processing personal data regarding them, except when the controller has a legal basis for the processing despite the prohibition. Data subjects have the right to request the removal of any personal data regarding them if the controller no longer has a legal basis to store the information.

### *9.4 Right to data portability*

Data subjects have the right to receive the personal data concerning them in a structured, commonly used and machine-readable format. As a general rule, data subjects have the right to transfer the details in question to another company or controller, *if* the data processing is based on consent or an agreement and the information is processed automatically by means of software of some kind.

Since the Company processes the personal data based on legitimate interest and statutory obligation instead of simple consent and agreement, such information (e.g. information necessary for invoicing) does not need to be disclosed. The obligation to disclose only applies to electronic information.

## 10. CONTACT INFORMATION

If you have any questions or comments regarding the data protection rules prepared by the Company or the Company's processing of personal data in general, please contact the person responsible for data protection matters using the contact details provided below.

Jukka Pirinen, Qridi Oy

info@qridi.fi