

## Qwarie Data Protection Compliance Statement

### Introduction

This is a statement of Data Protection compliance adopted by Qwarie Ltd. Qwarie recognises and accepts its responsibility as set out in the Data Protection Act 1998 and sub-legislation contained therein. We take all reasonable steps to meet this responsibility and to promote good practice in the handling and use of personal information. Also, and in the absence of legislation from HM Government concerning General Data Protection Regulation (GDPR), Qwarie has adopted EU Regulation 2016/679 of the European Parliament and of the Council, issued on 27 April 2016. This concerns the protection of natural persons with regard to the processing of personal data and the free movement of such data. GDPR is the minimum standard for data protection that comes into force on 25 May 2018.

This statement applies to all employees and individuals about whom we process personal information, as well as the customers who request our services.

### Scope

We collect and use information about people with whom we work in order to conduct our business and provide our services. All personal information, whether in paper, electronic or any other format, is handled and managed in accordance with data protection legislation.

We regard the lawful and correct treatment of personal information by Qwarie Ltd as very important to successful operations and to maintaining confidence between those with whom we deal with and ourselves. We ensure that our organisation treats personal information lawfully and correctly.

Qwarie Ltd. collects, stores and analyses two types of information. There is information we collect about our customers and there is information that we collect under instruction from our customers. For additional information, please revert to our Privacy Policy.

The following paragraphs provide a brief aid to current data protection legislation.

## Definitions

**Personal data** is defined as any information relating to an identified or identifiable natural person; an identifiable 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, etc.

**Sensitive personal data** is defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data, data relating to criminal offences and convictions.

**Data Subject** is defined as an individual who is the subject of the personal data, for example employees, customers, suppliers.

**Data Controller** is defined as the entity that determines the purposes, conditions and means of the processing of personal data.

**Data Processor** is defined as the entity that processes data on behalf of the Data Controller.

**Encrypted Data** is defined as personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access.

**Data Protection Principles**, which we fully endorse and adhere to. In summary, this means personal information must be:

1. Processed fairly, lawfully and in a transparent manner and, in particular, shall not be processed unless specific conditions are met;
2. Processed for limited, specific and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Adequate, relevant and sufficient for the purpose or purposes for which it is processed;
4. Accurate and, when necessary, kept up to date;
5. Kept for as long as necessary and no longer for that purpose or those purposes;
6. Processed in accordance with individuals' rights;
7. Kept secure; so that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Only transferred to a country or territory that ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

## Compliance (For additional information, please revert to our Privacy Policy)

Qwarie Ltd, through appropriate management, ensures strict application of criteria and controls:

- use personal information in the most efficient and effective way to deliver better services;
- observe fully conditions regarding the fair collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs to comply with any legal requirements;
- ensure the quality of the information used, including its accuracy and relevancy for the purpose specified;
- apply strict checks to determine the length of time the information is held;
- securely destroy data which is no longer needed;
- take appropriate technical and organisational security measures to safeguard personal information (including unauthorised or unlawful processing and accidental loss or damage of data);
- Qwarie considers encryption to be essential for the safe transfer and storage of information; By default, all data saved on Qwarie servers is encrypted. For additional information, please revert to our Security Policy.
- ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Act and the General Data Protection Regulation;

In addition, we take steps to ensure that:

- there is someone with specific responsibility for data protection in the company;
- queries about handling personal information are promptly dealt with;
- everyone managing and handling personal information is appropriately supervised;
- methods of handling personal information are clearly described;
- methods of handling personal information are regularly assessed and evaluated;

## Employee Responsibilities

Everyone who works for Qwarie has some responsibility for ensuring that data is collected, stored and handled appropriately and in line with data protection principles. We make certain that:

- the only people able to access personal data are those who need it for their duties;
- everyone managing and handling personal information is appropriately trained to do so;
- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- everyone managing and handling personal information is periodically reviewed by Qwarie managers, where each employee signs off on their compliance every three months;
- everyone managing and handling personal information keeps all data secure by taking the appropriate security precautions;
- Systems Administrator ensures all systems, services and equipment used for storing data meet the best security standards;
- Systems Administrator performs regular checks and scans to ensure security hardware and software is functioning properly,

## Disclosure

A copy of this statement will be brought to the attention of all employees. All employees are familiar with and comply with this statement at all times.

## Notification of changes to this statement

We are continually improving our methods of communication and our service. Because of these ongoing changes, changes in the law and the changing nature of technology, our data practices will change from time to time. If you wish to be notified of changes to this statement, please subscribe to our e-mail list.

## References

To acquire the fuller extent of our compliance, please revert to the following documents:

- Qwarie Privacy Policy
- Qwarie Security Policy
- Qwarie Data Breach Policy
- Qwarie Modern Slavery Policy
- Qwarie Customer Consent to Data Processing

To read or download our compliance documents, please go to <https://www.qwarie.com/documents>