Data Protection Policy

Contents

Description	Page No.
Introduction	2
Scope	2
Policy Statement	2
Privacy Policy – Data Protection Principles:	2
1. Processed lawfully, fairly and in a transparent manner	3
2. Collected for specified, explicit and legitimate purpose	4
3. Adequate, relevant and limited to what is necessary	4
4. Accurate and where necessary, kept up to date	4
5. Retained only for as long as necessary	4
6. Processed in an appropriate manner to maintain security	5
Demonstrating Compliance with GDPR's other Principles (Accountability)	6
Consent	6
Data Subjects Rights	6
Subject Access Requests	7
Security of Data	7
Retention and Disposal of Data	8
Data Flow	8
Data Protection Risks	9
1. Data Storage	9
2. Data Usage	9
3. Data Accuracy	10
4. Providing Information	10
Roles and Responsibilities	11
Definitions	12

April 2024.V1

Introduction

'Rize' needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled, stored and erased, to meet the company's data protection standards thus complying with the legislation.

Purpose

This data protection policy ensures 'Rize':

- complies with Data Protection legislation and follows good practice;
- protects the rights of employees, customers and partners;
- is transparent in terms of how it stores and processes individuals' data;
- protects itself from the risks associated with a data breach.

Scope

The General Data Protection Regulation 2016 (GDPR) replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e., living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Policy Statement

'Rize', located at Rize, Riverbank Cottages, Oldbridge, County Meath is committed to compliance with all relevant EU and Irish law in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information we collect and process in accordance with the (GDPR). We are committed to protecting and respecting personal data. We wish to be transparent on how we process personal data and demonstrate that we are accountable with the GDPR in relation to our processing of the data.

The GDPR describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Privacy Policy - Data Protection Principles

The GDPR is underpinned by six important principles requiring that personal data be:

1. **Processed lawfully, fairly and in a transparent manner;**
2. **Collected for specified, explicit and legitimate purpose;**
3. **Adequate, relevant and limited to what is necessary;**
4. **Accurate and where necessary, kept up to date;**
5. **Retained only for as long as necessary;**
6. **Processed in an appropriate manner to maintain security.**

The GDPR and this policy are applicable to all personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

'Rize' is responsible for reviewing the register of data processing annually, in light of any changes to 'Rize' activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments (DPIA's).

Partners and any third parties working with or for 'Rize', and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy.

No third party may access personal data held by 'Rize' without having first entered into a data confidentiality agreement which imposes obligations on the third party no less onerous than those to which we are committed, and which gives us the right to audit compliance with the agreement.

1. Personal Data must be processed lawfully, fairly and in a transparent manner

'Rize' will not process any personal data unless there is a legal basis to do so (under GDPR) such as consent, or it is necessary for the performance of a contract[1] .

Therefore, processing will be lawful if:

1. The 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; or
2. the data subject has given consent to the processing of his or her personal data for one or more specific purposes (e.g., for marketing purposes).

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement. See GDPR Regulation (EU) 2016/679. The GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using, clear and plain language.

The specific information that must be provided to the data subject must, as a minimum, include:

- the identity and the contact details of the controller and, if any, of the controller's representative;
- the contact details of 'Rize';
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the period for which the personal data will be stored;

[1] The other four lawful basis are in short; 1) legitimate interest, 2) it is necessary for compliance with a legal obligation, 3) it is in the public interest and 4) to protect the vital interests of the data subject.

- the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- also, where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

2. **Personal data can only be collected for specific, explicit and legitimate purposes**
   Data obtained for specified purposes must not be used for a purpose that differs

3. **Personal Data must be adequate, relevant and limited to what is necessary**
   'Rize' is responsible for ensuring that 'Rize' do not collect information that is not strictly necessary for the purpose for which it is obtained.

   All data collection forms, e.g., proposal forms/application forms (electronic or paper-based), must include a fair processing statement or link to a privacy statement and be approved by 'Rize'. Callers should be advised that the privacy statement is available on the website[2].

   'Rize' will ensure that, on an (annual) basis all data collection methods are reviewed by (internal audit/external experts) to ensure that collected data continues to be adequate, relevant and not excessive.

4. **Personal data must be accurate and kept up to date with every effort to erase or rectify without delay**
   Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

   'Rize' is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

   It is also the responsibility of the data subject to ensure that data held by 'Rize' is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

   'Rize' is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date taking into account, the volume of data collected, the speed with which it might change and any other relevant factors.

   On at least an annual basis, 'Rize' will review the retention dates of all the personal data processed by 'Rize', by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose.

2

5. **Personal data must be kept in a form such that the data subject can only be identified for as long as is necessary for processing.**
Where personal data is retained beyond the processing date, it will be minimised, encrypted/pseudonymised, in order to protect the identity of the data subject, in the event of a data breach.

Personal data will be retained in line with the Retention of Records Procedure/Schedule and, once its retention date has passed, it must be securely destroyed, as set out in this procedure.

'Rize' must specifically approve any data retention that exceeds the retention periods defined in the Retention of Records Procedure and must ensure that the justification is clearly identified, and in line with the requirements of the data protection legislation. This approval must be in written format.

6. **Processed in an appropriate manner to maintain security**
In determining appropriateness, 'Rize', should also consider the extent of possible damage or loss that might be caused to individuals (e.g., staff or customers) if a security breach occurs, the effect of any security breach on 'Rize' itself, and any likely reputational damage, including the possible loss of customer trust.

When assessing appropriate technical measures, 'Rize' will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- Privacy enhancing technologies such as pseudonymisation and anonymisation; and

When assessing appropriate organisational measures, 'Rize' will consider the following:

- The appropriate training levels throughout 'Rize';
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper-based records;
- Adoption of a clear desk policy;
- Storing of paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employees own personal devices being used in the workplace;
- Adoption of clear rules about passwords;
- Making regular backups of personal data and storing the media off-site; and
- Taking appropriate security measures when transferring data outside the EEA and the imposition of contractual obligations on the importing organisations.

These controls have been selected, based on identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

Demonstrating compliance with the GDPR's other Principles (Accountability)

The GDPR includes provisions that promote accountability and governance. These compliment the GDPR's transparency requirements. The accountability principle in Article 5(2) requires 'Rize' to demonstrate that we comply with the principles and states explicitly that this is our responsibility.

Consent

'Rize' understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

'Rize' also understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the grounds of misleading information will not be a valid basis for processing.

There must be some active communication between the parties to demonstrate "active consent". Consent cannot be inferred from non-responsive communications. We must be able to demonstrate that consent was obtained for the processing operation.

For sensitive data, explicit consent from data subjects must be obtained unless an alternative legitimate basis for processing exists.

Data Subjects' Rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed;
- To prevent processing likely to cause damage or distress;
- To prevent processing for purposes of direct marketing;
- To be informed about the mechanics of automated decision-making process that will significantly affect them;
- To not have significant decisions, that will affect them, taken solely by automated process;
- To sue for compensation if they suffer damage by any contravention of the GDPR;
- To act to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data;
- To request the Data Protection Commissioner to assess whether any provision of the GDPR has been contravened;
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller;

- To object to any automated profiling that is occurring without consent.

Data Subject Access Requests

All individuals who are the subject of personal data held by 'Rize' are entitled to:

- Ask **what information** the company holds about them and why;
- Ask **how to gain access** to it;
- Be informed about **how to keep it up to date**;
- Be informed about how the company meets **its data protection obligations**.

Should an Individual contact the company requesting this information, this is called a Subject Access Request.

Subject Access Requests from individuals should be made by email, if possible, addressed to 'Rize' at cara@rise.ie 'Rize' can supply a standard request form, although individuals do not have to use this.

We will aim to provide the relevant data within **30 days**. Where we are unable to provide the requested data to the data subject within 30 days, we will advise the data subject and provide the reason why.

We will always verify the identity of anyone making a subject access request before handing over any information.

Security of Data

All Employees/Staff are responsible for ensuring that any personal data that 'Rize' holds and for which we are responsible, is kept securely and is not, under any conditions, disclosed to any third party unless that third party has been specifically authorised by 'Rize' to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy.

All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with Company Policy; and/or
- stored on (removable) computer media which are encrypted in line with the Data Deletion Register.

Care must be taken to ensure that PC screens and terminals are not visible except to authorised employees/staff of 'Rize'. All employees/staff are required to enter into a Confidentiality Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs etc.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with our policies, provided that this removal does not infringe our other legal responsibilities and obligations. Personal data may only be deleted or disposed of in-line with the data retention period listed in our Privacy Policy.

Records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed, as required before disposal.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

Retention and Disposal of Data

'Rize' shall not retain personal data for a longer period than is necessary, in relation to the purpose(s) for which the data was originally collected, except where it is required to be retained to meet other legislative or regulatory obligations.

'Rize' may also store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

Personal data must be disposed of securely, in accordance with the sixth principle of the GDPR. Thus, processed in an appropriate manner, to maintain security, thereby, protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the data retention period listed in our Privacy Policy.

Data flow

'Rize' has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance regime namely;

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of 'Rize' throughout the data flow;
- key systems and repositories;
- any data transfers;

- all retention and disposal requirements.

'Rize' assesses the level of risk to individuals associated with the processing of their personal data. 'Rize' will manage any risks identified by the risk assessment, to reduce the likelihood of a non-conformance with this policy.

Where a type of processing, particularly using new technologies and considering the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, we will, prior to the processing, carry out a Data Protection Impact Assessment (DPIA) on the impact the envisaged processing operations will have on the protection of personal data. A single Data Protection Impact Assessment (DPIA) may address a set of similar processing operations that present similar high risks.

Data Protection Risks

This policy helps to protect 'Rize' from potentially, serious data security risks, including:

- **Breaches of confidentiality:** for instance, information processed inappropriately;
- **Reputational damage:** for instance, the Company could suffer material or non-material damage if hackers successfully gained access to sensitive data.

1. **Data Storage**

   These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or Data Controller. When data is **stored in paper format,** it should be kept in a secure place where unauthorised people cannot see it.

   These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

   - When not required, the paper or files should be kept **in a locked drawer or filing cabinet**;
   - Employees should make sure paper, and printouts are **not left where unauthorised people could see them**, like on a printer;
   - **Data printouts should be shredded** and disposed of securely when no longer required;
   - When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts;
   - Data should be **protected by strong passwords** that are changed regularly and never shared between employees;
   - If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used;
   - Data should only be stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing service.**
   - Servers containing personal data should be **sited in a secure location**, away from general office space.
   - Data should be **backed up frequently**. Those back-ups should be tested regularly, in line with the company's standard backup procedures.
   - Data should **never be saved directly** to mobile devices like tablets or smart phones.
   - All servers and computers containing data should be protected by **approved security software and a firewall**.

2. **Data Usage**

Personal data is of no value to 'Rize' unless the business can make use of it. However, it is when personal data is accessed and used, that it can be at the greatest risk of loss, corruption or theft. For example:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. It should never be sent by email (unless it is encrypted or pseudonymised), as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area (EEA) without the knowledge and consent of 'Rize' and then only where there is an appropriate "level of protection for the fundamental rights of the data subjects" (adequacy decision or SCCs/BCRs).
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

3. Data Accuracy

The law requires 'Rize' to take reasonable steps to ensure data is kept accurately and up to date. The higher the importance, that the personal data is accurate, the greater the effort 'Rize' should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps, to ensure it is kept as accurate and up to date as possible:

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets;
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call;
- 'Rize' will make it **easy for data subjects to update the information** we hold about them. For instance, via the company website;
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database:

4. Providing Information

'Rize' aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How their data is being used;
- How to exercise their rights.

To this end, the company has a Privacy Policy setting out how data relating to individuals is used by the company.
General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**;
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers;

- 'Rize' **will provide training** to all employees to help them understand their responsibilities when handling data;
- Employees should **keep all data secure**, by taking sensible precautions and following the guidelines below;
- **Strong passwords are mandatory,** and they should never be shared;
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated.** If it is found to be out of date and/or no longer required, it should be deleted and disposed of appropriately.
- Employees **should request help** from their line manager or 'Rize' if they are unsure about any aspect of data protection.

Roles and Responsibilities

'Rize' is a Data Controller and/or Data Processor under the GDPR.

'Rize' has specific responsibilities in respect of data protection policies and procedures and is the first point of call for employees/staff, seeking clarification on any aspect of data protection compliance.

All Employees/Staff
Management and all those in managerial or supervisory roles throughout 'Rize' are responsible for developing and encouraging good information handling practices within 'Rize'; responsibilities are set out in individual job descriptions. Compliance with data protection legislation is the responsibility of all employees/staff of 'Rize' who process personal data.

Employees/staff of 'Rize' are responsible for ensuring that any personal data about them and supplied by them to 'Rize' is accurate and up to date.

Everyone who works for or with 'Rize' has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following have key areas of responsibility:

- Cara Driscoll is ultimately responsible for ensuring that 'Rize' meets its legal obligations.
- Cara Driscoll is responsible for:
    - Keeping all interested parties updated about data protection responsibilities, risks and issues;
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule;
    - Arranging data protection training and advice for the people covered by this policy;
    - Handling data protection questions from staff and anyone else covered by this policy;
    - Dealing with requests from individuals to see the data 'Rize', holds about them (also called 'Data Subject Access Requests').

- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

Staff awareness training is mandatory for anyone who handles personal data or who is responsible for overseeing data protection practices.

'Rize' will also ensure that training is relevant to the work that employees do. For example, those responsible for processing personal data should be taught about their responsibilities and the threats that come with that.

Definitions

Definitions used by the company drawn from the General Data Protection Regulation (GDPR)

Personal Data

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 Subject

Any living individual who is the subject of personal data held/processed by our organisation.

Processing

Any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means or not, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal Data Breach

A breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data Subject Consent

Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Contacts

GDPR Owner, Cara Driscoll CEO of Rize cara@rize.ie

Policy Review

- Policy Prepared for: **'Rize'**
- Approved by Management On: **22/05/2025**
- Policy Became Operational on: **12/11/2024**
- Next Review Date: **22/05/2026**