Rialto Development Association

Data Protection Policy

Contents

1. Purpose 2
2. Scope 2
3. Associated Documents 2
4. Roles and Responsibilities 2
5. Policy Objectives 3
6. Compliance with Major Principles 4
   6.1 Transparency, Purpose and Lawful Basis for Processing 4
   6.2 Purpose Limitation 4
   6.3 Data Minimisation 4
   6.4 Accuracy and Quality 4
   6.5 Retention and Storage Limitation 4
   6.6 Security and Confidentiality 4
7. Our Obligations as a Data Controller 4
   7.1 Privacy Notice 4
   7.2 Record of Processing Activities (RoPA) 5
   7.3 Data Breaches 5
   7.4 Contracts with Data Processors 5
   7.5 Data Subject Rights 5
   7.6 Data Protection Impact Assessment 5
   7.7 Data Protection Officer 5
   7.8 Overseas Transfer 5
8. Audits and Monitoring 6
9. Training 6
Appendix 1 – Glossary of Data Protection Terms 7
Appendix 2 - Data Protection Principles 8

1. Purpose

The purpose of this policy is to set out Rialto Development Association's (RDA) commitment to personal data protection and to outline the arrangements RDA has made to meet its legal obligations to protect the personal data and by extension the privacy of the people whose data it processes.

This policy also serves as a reference document for employees and third parties on the responsibilities associated with processing personal data.

RDA's activities comprise a number of projects so this policy applies to RDA's Community Services Programme (CSP), Rialto Community Drug Team (RCDT), Rialto Youth Project (RYP), Rialto Day Care Centre, Rialto Community Network (RCN) and the Community Employment (CE) Scheme operated by RDA.

2. Scope

This policy applies to the processing by or on behalf of RDA projects of personal data on natural persons (data subjects). The policy is designed to ensure that RDA complies with its obligations under the General Data Protection Regulation, other relevant data protection laws notably the Data Protection Acts 1988-2018, and codes of conduct (herein collectively referred to as "the data protection laws") operable in Ireland.

The policy is binding on all trustees and employees of RDA along with third party data processors and service providers that support RDA in the processing of personal data. **Adherence to this policy is mandatory and non-compliance could lead to disciplinary action against employees in accordance with contracts of employment or termination of service contracts in the case of service providers.**

3. Associated Documents

Reference	Document Type	Document Title
A	**Register**	Register of Processing Activity
B	**Notice**	Privacy Notice
C	**Procedure**	Retention of Personal Data
D	**Procedure**	Dealing with Requests from Data Subjects
E	**Work Instruction**	Dealing with Requests to Access or Receive Data
F	**Form**	Data Subject Request Form
G	**Register**	Data Subject Request Log
H	**Procedure**	Assessing and Reporting a Data Breach
I	**Form**	Data Breach Incident Report
J	**Register**	Data Breach Incident Log
K	**Procedure**	Data Processor Services
L	**Procedure**	Conducting a Data Protection Impact Assessment

4. Roles and Responsibilities

In relation to the governance of our data protection policies and processes RDA has:

- Assigned leadership and management responsibility for data protection in RDA.
- Allocated responsibility for data protection compliance and ensured that the designated person(s) has(ve) sufficient access, support and resources to perform the role.
- Educated employees and volunteers about the requirements under the data protection legislation, the benefits of applying good personal data management practices and the potential implications of non-compliance.

- Provided effective data protection training for all employees and volunteers consistent with their roles.

Responsibility for Data Protection - Summary

Board	Approve the Data Protection Policy and oversee implementation of good data protection management practices Identify and manage risks associated with failure to implement the policy if not appropriately managed. Allocate responsibilities and provide sufficient resources. Lead by example: make data protection a priority and incorporate it into board and management systems and processes.
Centre Manager	Responsible for compliance with data protection legal requirements, and championing good data protection practices in the organisation and among service projects that operate in St. Andrew's Community Centre.
Project Manager	Each Project Manager is responsible for complying with this policy and compliance with data protection requirements in respect of the personal data processed by the project. RDA will assist projects in meeting their obligations by providing templates for and guidance on the processing of personal data but compliance is a matter for each project. The Project Managers should also champion good data protection policies for their project.
Employees and Volunteers	All staff and volunteers are responsible for familiarising themselves with the policy and ensuring that any data that they handle is processed in accordance with this policy and related procedures. In particular, employees and volunteers have a role to play in ensuring that personal data that they use in their work is kept secure and confidential. Employees and volunteers are responsible for reporting any potential breach or loss of personal data for which they are responsible or become aware of to their Project Manager.

5. Policy Objectives

RDA Projects process personal data in the course of providing services to clients and service users of St. Andrew's Community Centre, and supporting the volunteers and employees who are engaged in providing those services.

Protecting the privacy of Data Subjects by ensuring and maintaining the security and confidentiality of personal and/or special category data is a compliance priority for RDA.

Our data protection objectives are to:

- Ensure that individuals who entrust us with their personal data feel confident that they will be handled in accordance with their rights under data protection laws;

- Ensure that all employees and service providers involved in processing personal data are competent and knowledgeable about our data protection obligations and how they apply to their specific roles within RDA;
- Enhance RDA'S reputation as a reputable, trustworthy organisation which is committed to high standards of compliance and ethical behaviour;
- Minimise as far as possible the legal, financial or reputational risks to RDA that can arise from processing personal data.

6. Compliance with Major Principles

The principles of personal data management as described in GDPR are detailed in Appendix 2. In summary, these principles to which RDA adheres are as follows:

6.1 Transparency, Purpose and Lawful Basis for Processing

RDA advises all Data Subjects about what data it collects, what it is used for, who it might be shared with, where and for how long it may be retained, and how it is secured in addition to other relevant details about processing personal data. We also advise data subjects of their rights, where to get further information and how to make a complaint.

RDA establishes the purpose and lawful basis for processing before processing any personal data.

6.2 Purpose Limitation

RDA processes personal data only for the stated purpose or for purposes that are compatible with the original purpose. If processing for an incompatible process is contemplated, we seek the consent of the Data Subject before processing the data for the new purpose.

6.3 Data Minimisation

RDA only ever obtains, retains, processes, and shares the minimum amount of personal data that is essential for carrying out our services and/or meeting our legal obligations.

6.4 Accuracy and Quality

RDA takes steps to ensure the accuracy and quality of personal data processed and acts to rectify any inaccuracies where they occur.

6.5 Retention and Storage Limitation

RDA retains and stores personal data only for as long as is necessary for the purpose for which the data is processed.

6.6 Security and Confidentiality

RDA has adequate and appropriate technical and organisational measures commensurate with the risk to the Data Subjects to ensure the security and maintain the confidentiality of personal data processed.

7. Our Obligations as a Data Controller

In addition to complying with the above principles of personal data management RDA recognises that it has specific obligations as a Data Controller. These obligations, and the measures taken or planned to address them, are:

7.1 Privacy Notice

Where personal data is obtained directly from the individual we provide the Data Subject with a Privacy Notice (Ref. B) setting out the identity and the contact details of the controller, the contact

details of our Centre Manager, the purpose(s) and legal basis for the processing, the existence of the rights of data subjects and how to exercise them, the right to lodge a complaint with the Supervisory Authority and other information as required by law.

7.2 Record of Processing Activities (RoPA)

RDA maintains a record of personal data processing activities in its office (Ref. A).

7.3 Data Breaches

RDA has extensive technical and organisational security measures in place to protect the security and confidentiality of personal data. However, RDA recognises that breaches i.e. unauthorised release of, or access to, personal data can occur. RDA understands and has procedures to assess, record and, where appropriate, notify the Data Protection Commission and/or the Data Subject, In the event that a breach occurs, refer to ***Assessing and Reporting a Data Breach Procedure*** (Ref. H). See also Data Breach Incident Report (Ref. I) and Data Beach Incident Report Log (Ref. J).

7.4 Contracts with Data Processors

RDA contracts with external data processors to provide certain services that entail the processing of personal data e.g. IT Systems and Services.

RDA assesses potential service providers carefully and engage only processors who have measures in place to process personal data appropriately on behalf of RDA. All processing of personal data is subject to having a properly constituted Data Processing Agreement in place. See (Ref K) procedure for Engaging Services of a Data Processor.

7.5 Data Subject Rights

RDA understands and upholds the rights of Data Subjects under Data Protection Law and has arrangements in place to ensure that these rights are understood by employees and volunteers who process personal data and to respond to requests in a timely fashion. See Procedure for Handling Data Subject Requests (Ref. D), the Data Subject Request Form (Ref. F) and the Data Subject Request Log (Reg. G).

7.6 Data Protection Impact Assessment

Where RDA processes, or is considering the processing of, personal data utilising new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, RDA carries out a Data Protection Impact Assessment (DPIA). See procedure for Conducting a Data Protection Impact Assessment (Ref. L).

7.7 Data Protection Officer

RDA has assessed whether it meets the criteria requiring the appointment of a Data Protection Officer (DPO) and has concluded that a DPO is not required. Overall responsibility for data protection has been assigned to the Centre Manager while Project Managers have specific responsibilities in respect of their projects (see table on p. 3).

7.8 Overseas Transfer

RDA is aware of its obligations to safeguard personal data transferred to third countries.

8. Audits and Monitoring

RDA carries out regular audits and compliance monitoring with a view to ensuring that our measures and controls to protect personal data are effective and compliant.

The respective Manager of each service project has overall responsibility for assessing, testing, reviewing, and improving the processes, measures and controls in place and reporting improvement action plans to their respective project management committee as appropriate.

9. Training

RDA provides training for employees and volunteers in relation to data protection, the content of which is tailored to the requirements of their roles and the extent to which they are involved in processing personal data.

Staff who process personal or special category information are provided with extensive data protection training and other continuing professional development and mentoring as appropriate.

Appendix 1 – Glossary of Data Protection Terms

"Consent" of the data subject means 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 e.g. by applying online for a job, signifies agreement to the Processing of personal data relating to him or her.

"Data controller" means, the natural or legal person, public authority, agency or other body in this case RDA which, alone or jointly with others, determines the purposes and means of the Processing of personal data.

"Data processor" means a natural or legal person, public authority, agency or other body which Processes personal data on behalf of the controller.

"Data protection laws" means for the purposes of this document, the collective description of the GDPR and any other relevant data protection laws that RDA complies with.

"Data subject" means an individual who is the subject of personal data.

"GDPR" means the *General Data Protection Regulation (EU) (2016/679).*

"Personal data" is *"any information relating to an identified or identifiable natural person"* and includes *(but is not limited to),* name, address, email address, data of birth, IP address, identification numbers, bank details along with special categories of personal data as defined below.

"Processing" or "Process" 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, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"'Special Categories of Personal Data' are data relating to *"racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"*

Appendix 2 - Data Protection Principles

The ***General Data Protection Regulation (GDPR) (EU)2016/679)*** was approved by the European Commission in April 2016 and applies in all EU Member States from 25th May 2018. As a '*Regulation*' rather than a '*Directive*', its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As RDA Processes personal information regarding individuals (*data subjects*), we are required under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles. RDA has additional responsibilities under the Data Protection Acts 1988-2018.

Article 5 of the GDPR requires that personal data shall be: -

- ***a)*** Processed lawfully, fairly and in a transparent manner in relation to the data subject ***('lawfulness, fairness and transparency')***
- ***b)*** collected 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ***('purpose limitation')***
- ***c)*** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimisation')***
- ***d)*** accurate and, where necessary, kept up to date; 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')***
- ***e)*** 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation')***
- ***f)*** 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').***

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection principles* ***('accountability')*** and requires that firms ***show how*** they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.