
	POLICY		Page: 1 of 9
	Data Protection Privacy Policy		Date: 04/01/2022
	DPOL-1	Issue: 1	Approval: Ronan Corrigan

Contents

1. INTRODUCTION.....	2
2. DEFINITIONS.....	2
3. PURPOSE	3
4. SCOPE	3
5. RESPONSIBILITY.....	3
6. POLICY	3
General:.....	3
Records of Processing Activities	3
Data Processor Agreements:	4
Data Access Requests:	4
Data Breaches:	5
Data Protection Impact Assessments:	6
Registration with the Data Protection Commissioner:	6
Appendix A – Information Security Policy	7
Appendix B – DPIA Process	9

	POLICY		Page: 2 of 9
	Data Protection Privacy Policy		Date: 04/01/2022
	DPOL-1	Issue: 1	Approval: Ronan Corrigan

1. INTRODUCTION

Data Protection is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data. Rosata Recruitment Limited, or “the Company”, as part of its ongoing business, collects and uses personal data about its employees and, to the extent necessary, its clients, candidates and other individuals. These individuals, or ‘data subjects’, have privacy rights in relation to the processing of their personal data as subject to regulations and legislation.

In establishing this policy, Rosata Recruitment Limited refer to the seven key principles as set out in Article 5 (‘Principles relating to processing of personal data’) of the GDPR; they are, in summary:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability.

Rosata Recruitment Limited is committed to complying with these key principles and with its Data Protection obligations at large.


2. DEFINITIONS

‘Data Protection Acts’ means the Data Protection Acts 1988 to 2018 and the European General Data Protection Regulation (“GDPR”) as amended, modified or consolidated.

Definitions of ‘personal data’, data ‘processing’, data ‘controller’, data ‘processor’, ‘third party’, ‘consent’, and ‘personal data breach’, as given in Article 4 (‘Definitions’) of the GDPR, shall apply.

‘Special categories of personal data’ receive greater protection under the Data Protection Acts and refers to data falling under the following categories:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Data concerning health
- Data concerning a person’s sex life or sexual orientation
- Genetic data
- Biometric data

	POLICY		Page: 3 of 9
	Data Protection Privacy Policy		Date: 04/01/2022
	DPOL-1	Issue: 1	Approval: Ronan Corrigan

3. PURPOSE

This policy is a statement of the commitment of Rosata Recruitment Limited to protect the rights and privacy of individuals in accordance with the Data Protection Acts.

The purpose of this policy is to demonstrate the Company's transparency and accountability in the processing of personal data, with focus on safeguarding the rights of the data subject.

4. SCOPE

This policy applies to all personal data created or received in all formats in the course of the business of Rosata Recruitment Limited, including clients, candidates, service end users, suppliers, and other third parties as they may relate.

Personal data may be communicated verbally, or it may be held or transmitted in hardcopy format, such as paper of physical records, or electronic formats.

This policy applies to all persons employed by Rosata Recruitment Limited and those persons providing services to the Company which in any way may involve the processing of personal data.

5. RESPONSIBILITY

The Managing Director has overall responsibility for ensuring compliance with the Data Protection Acts.

Employees and any subcontractors working for the Company are advised of their responsibility in exercising due diligence in:

- Receiving, verifying and relaying data access requests to the Managing Director
- Identifying and reporting data breaches to the Managing Director

6. POLICY

General:


In general, Rosata Recruitment Limited shall take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of all personal data no matter the format.

The Information Security Policy, as laid out in Appendix A, shall refer.

Records of Processing Activities

In order to maintain documentation on processing activities as both a data controller and a data processor, and with reference to Article 30 ('Records of processing activities') of the GDPR, the Company maintains a Personal Data Inventory. The Inventory details:

- The party that is subject to data processing
- Description of the particular personal data which is being processed
- The justification for why the personal data is being held

	POLICY		Page: 4 of 9
	Data Protection Privacy Policy		Date: 04/01/2022
	DPOL-1	Issue: 1	Approval: Ronan Corrigan

- The manner in which the personal data was or is obtained
- The justification for why the personal data was gathered
- The stated retention period for the personal data
- The known security measures in place to secure the personal data
- The basis of bases upon which the personal data is shared with third parties, if applicable
- The legal basis or bases upon which processing of the personal data is justified
- The use of third parties, if any, including:
 - The third party with whom the personal data is shared
 - Description of the particular personal data which is shared
 - The justification for why the personal data is shared
 - The corresponding data processing activities undertaken by the third party
 - The known security measures in place during the transfer of the personal data
 - The known security measures in place with the third party
 - The basis or bases upon which Rosata Recruitment Limited assess or ensure the security of personal data with the third party.

Data Processor Agreements:


Where Rosata Recruitment Limited, in the role of a data controller, avail of the services of a third party as a data processor, a Data Processor Agreement or similar contract shall be in place between both parties. In accordance with Article 28 ('Processor') of the GDPR, the Agreement or contract shall set out:

- The subject matter and duration of the data processing
- The nature and purpose of the data processing
- The type of personal data and categories of data subjects
- The obligations and rights of the data controller, as per Article 28.

Data Access Requests:

Data subjects are entitled to make an access request under the Data Protection Acts for a copy of their personal data and for information relating to that data. This shall be complied with within one calendar month. The information released under the access request includes:

- The nature of the personal data
- The purposes for which the personal data is processed
- The period for which the personal data is processed
- The recipients of the personal data
- Whether the personal data has been or will be transferred outside of the European Union
- The logic involved in any automatic personal data processing and automated decision making and, when based on profiling, the consequences of such data processing.

	POLICY		Page: 5 of 9
	Data Protection Privacy Policy		Date: 04/01/2022
	DPOL-1	Issue: 1	Approval: Ronan Corrigan

The data subject shall also be informed of their right to request rectification or deletion of the personal data, and the right to make a complaint to the Data Protection Commissioner.

In certain circumstances, the Company is able to avail of exemptions from the restrictions in the Data Protection Acts (e.g., disclosure required by law), or where justifiable in accordance with the Data Protection Acts, apply a chargeable fee for the release of personal data.

Where data access is refused, the data subject is advised of their right of complaint to the Data Protection Commissioner.

Data Breaches:

Where a potential data breach has occurred, the matter shall be reported to the Managing Director without delay. All employees, subcontractors and third-party data processors are notified of their obligations to report under contract, Agreement and/or training.

Potential data breaches shall be investigated fully by the Managing Director. Where it is found that a data breach has occurred, the breach shall be reported to the Data Protection Commissioner without undue delay and within 72 hours of its occurrence. Reporting to the Data Protection Commissioner shall include:


- The nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned
- The name and contact details of the contact point where more information can be obtained
- The likely consequences of the data breach
- The measures taken or proposed to address the data breach, including, where appropriate, measures to mitigate any possible adverse effects.

If a data breach is likely to bring harm to an individual, including the data subject (such as identity theft or confidentiality breach), this breach shall be reported to the individual or individuals concerned. In certain circumstances, this communication shall not be required:

- Where the Company has ensured encryption or some other form of protection where the data has been rendered unintelligible
- Where the Company has ensured that the high risk to the rights and freedoms of data subjects is no longer likely to materialise
- Where communication would involve disproportionate effort, and a public communication or similar would inform data subjects in an equally effective manner.

Where the data subject is to be notified, the communication shall be in clear and plain language and shall, at least:

- The nature of the personal data breach

	POLICY		Page: 6 of 9
	Data Protection Privacy Policy		Date: 04/01/2022
	DPOL-1	Issue: 1	Approval: Ronan Corrigan

- The name and contact details of the contact point where more information can be obtained
- The likely consequences of the personal data breach
- The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Data Protection Impact Assessments:

Where data processing is likely to result in a high risk to the rights and freedoms of natural persons, a Data Protection Impact Assessment, or DPIA, shall be carried out. Particular consideration shall be given where special categories of personal data is concerned.

The DPIA shall be carried out with reference to the iterative process laid out in Appendix B.


Registration with the Data Protection Commissioner:

At all times, Rosata Recruitment shall refer to guidance issued by the Data Protection Commissioner (DPC).

As part of its services, Rosata Recruitment may be required to register with the DPC as a Data Controller or Data Processor. Details of this registration shall be outlined below.

DPC Registration

Organisation Name:	Rosata Recruitment Limited
Registration Number	0009000701

	POLICY		Page: 7 of 9
	Data Protection Privacy Policy		Date: 04/01/2022
	DPOL-1	Issue: 1	Approval: Ronan Corrigan

Appendix A – Information Security Policy

INFORMATION SECURITY POLICY

1. PURPOSE

To ensure that Rosata Recruitment Limited do not contravene the Data Protection Acts and to ensure appropriate security measures are in place to prevent an actual or potential data breach.

2. SCOPE

This policy applies to all activities and personnel within, or providing services on behalf of, Rosata Recruitment Limited.

This policy concerns both hardcopy data and electronic data.

3. RESPONSIBILITY


The Managing Director is responsible for the implementation of this policy. The Managing Director shall consult with approved third-party IT providers and data protection advisors, as appropriate, towards ensuring the adequacy of security measures.

Employees, doctors, and any subcontractors working for Rosata Recruitment Limited are obliged to be aware and in act in accordance with this policy.

4. POLICY

4.1. Hardcopy Data:

The retention of hardcopy personal data should be minimised. Where hardcopy data retention is required, such as when mandated by legal requirements, the hardcopy shall be held in locked cabinets with access only permitted by the Managing Director or authorised delegate. These cabinets are located in offices with restricted access both during and outside business hours.

	POLICY		Page: 8 of 9
	Data Protection Privacy Policy		Date: 04/01/2022
	DPOL-1	Issue: 1	Approval: Ronan Corrigan

4.2. Electronic Data:

Electronic data shall be protected by antivirus software, firewalls and data encryption technology. Multi-factor authentication (MFA) shall be employed. All security measures shall be maintained and updated, as appropriate.


The recommended password protection policy is as follows:

- a) Minimum of twelve characters
- b) At least two of the following:
 - i) Upper-Case and Lower-Case letters; (A, a, Z, z)
 - ii) Numbers (0-9)
 - iii) Symbols (e.g., &, *, @, €, \$)
 - iv) Punctuation (?, “, !)

Devices shall enable and utilise Device Encryption, BitLocker or a similar means of encryption depending on the device and native operating system.

Flash drives or memory sticks shall not be used except in exceptional circumstances, with permission sought from, and provided by, the Managing Director.

Security measures shall be reviewed from time to time, having regard for the technology available, the cost, and the risk of unauthorised access.

	Policy		Page: 9 of 9
	Data Protection Privacy Policy		Date: 04/01/2022
	DPOL-1	Issue: 1	Approval: Ronan Corrigan

Appendix B – DPIA Process

