RELIANCE
SOCIAL HOUSING
GENERATE | AQUIRE | DEPLOY

Policy Control	
Policy Name	Data Protection Policy
Policy Owner	Chief Executive
Author	Andria Andreou - HR Manager
Version No.	1
Approved by Chief Executive	October 2023
Approved by Board	April 2024
Date of Implementation	April 2024
Date of Last Review	October 2023
Date of Next Review	October 2025
Published on Website	No

RELIANCE SOCIAL HOUSING
GENERATE | AQUIRE | DEPLOY

CONTENTS

1. Introduction

1.1. This policy is implemented pursuant to the provisions of the Data Protection Act 2018 and is designed to safeguard the data interests of all parties including, employees, workers, third parties, regulators etc.

2. Purpose

2.1. This policy outlines the scope of the DPA provisions in simple terms and informs all parties of their duties in respect of compliance with the DPA provisions and what to do should there be a data protection breach.

3. Scope

3.1. The policy includes in its scope all date which we process either in hardcopy or digital copy, this includes special categories of data.

3.2. This policy applies to employees, whether permanent or temporary, workers, contractors and all third parties (either new or existing).

4. Definition

TERM	MEANING
GDPR	General Data Protection Regulation
Data Controller	means a person who (either alone or. jointly or in common with other persons) determines the. purposes for which and the manner in which any personal **data**. are, or are to be processed. This applies to the Company and its employees
Data Processor	means any person (other than an employee of the data controller) who processes the data on behalf of the data controller i.e.., HR Payroll, IT services
Register of Interests	means a register of all systems or contexts in which personal data is processed by the Company

5. Duties & Responsibilities

5.1. Responsibilities of the Chief Executive - The Chief Executive will have overall responsibility for the strategic and operational running of the Company, including ensuring that all policies and processes comply with legal and regulatory guidelines. The responsibility for the maintenance, implementation, and application of these policies, will be delegated where necessary, to either the HR Manager or relevant departmental heads.

5.2. Responsibilities of Managers – Managers must ensure they have completed the data protection training module and are fully aware of the potential ramifications of a data

protection breach. They must ensure all employees are fully aware of these ramifications, which could lead to serious financial loss and/or significant reputational harm.

5.3. Responsibilities of Employees – All employees must ensure they have reviewed this policy as well as completed the data protection training module. They are regarded as data controllers as they work for the Company and in the event of a data protection breach it is crucial that a line manager and/or Chief Executive is notified immediately so that appropriate measures can be taken, in accordance with the DPA rules. The Company reserves the right to invoke the Company's Disciplinary procedure in cases involving serious data breaches, which have caused or are sufficiently likely to cause significant business harm.

6. Data Protection Principles

6.1. Reliance is committed to processing data in accordance with its responsibilities under the GDPR.

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

6.2.1. Processed lawfully, fairly and in a transparent manner in relation to individuals;

6.2.2. Collected for specified, explicit and legitimate purposes and further processed in a manner that is incompatible with those purposes; further processing for archiving purposes shall not be considered to be incompatible with the initial purposes;

6.2.3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;

6.2.4. 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;

6.2.5. 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 subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals.

6.2.6. Proceed 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.

7. General provisions

7.1. This policy applies to all personal data processed by the Company.

7.2. The Responsible Person shall take responsibility for the Company's ongoing compliance with this policy.

7.3. This policy shall be reviewed at least annually.

7.4. The Company shall register with the Information Commissioner's Office as an organisation that processes personal data.

8. Lawful, Fair, and Transparent Processing

8.1. To ensure its processing of data is lawful, fair, and transparent, the Company shall maintain a Register of Systems.

8.2. The Register of Systems shall be reviewed at least annually.

8.3. Individuals have the right to access their personal data and any such requests made to the Company shall be dealt with in a timely manner (see Handbook for further details of access of employee data).

9. Lawful purposes

9.1. All data processed by the Company must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).

9.2. The Company shall note the appropriate lawful basis in the Register of Systems.

9.3. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

9.4. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Company's systems.

10. Data minimisation

10.1. The Company shall ensure that personal data are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

11. Accuracy

11.1. The Company shall take reasonable steps to ensure personal data is accurate.

11.2. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date. All reasonable steps 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;

11.3. The Company shall use its best endeavours to ensure all Company reporting and retention systems are reviewed regularly to enable it to conduct checks for inaccuracies when necessary.

12. Archiving /Removal

12.1. To ensure that personal data is kept for no longer than necessary, the Company shall put in place a retention policy for each area in which personal data is processed and review this process annually.

12.2. The archiving policy shall consider what data should/must be retained, for how long, and why.

13. Security

13.1. The Company shall ensure that personal data is stored securely using modern software that is kept-up to date.

13.2. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

13.3. When personal data is deleted, this should be done safely such that the data is irrecoverable.

13.4. Appropriate back-up and disaster recovery solutions shall be in place.

14. **Data breaches**

14.1. All employees must understand what constitutes a data breach and should have completed the data protection training on commencement of employment.

14.2. In the event of a data protection breach the incident will need to be escalated to the Chief Executive immediately, so that an internal decision can be made as to whether to notify the ICO.

14.3. A written statement surrounding the data that has been disclosed used in contravention of the data protection principles will need to be compiled by a responsible manager and presented to the Chief Executive within 24hours. The Chief Executive shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website). The CEO will also need to consider whether the breach needs to be notified to the data subject as a matter of urgency.

14.4. The Company is obligated to report personal data breaches to the ICO in the following circumstances:

14.4.1. a breach of security leads to the destruction, loss, alteration, unauthorised disclosure of (or access to) personal data

14.4.2. Where the breach is likely to result in a risk to the rights and freedoms of individuals (where this risk is high, the Company must also notify the individuals concerned)

14.5. The report to the ICO must be made within 72 hours of the DC finding out about the breach.