Alderney Housing Association	Policy No. 023

Data Protection Policy

1. Context and overview

1.1. Introduction

The Alderney Housing Association (AHA) is a limited company registered in Alderney. The AHA provides social rented housing and partial ownership for local Alderney people whose needs cannot be met in the local housing market.

This policy describes how personal data must be collected, handled and stored to meet the AHA data protection standards and the requirements of the Bailiwick of Guernsey data protection legislation.

1.2. Why this policy exists

This data protection policy ensures the AHA:

- complies with all applicable data protection legislation and follows good practice
- protects the rights of employees, clients and shareholders
- is open about how it stores and processes individuals' personal data
- protects itself from the risks of a data breach.

1.3. Data protection legislation and registration

The Guernsey Data Protection (Bailiwick of Guernsey) Law 2017 incorporates the requirements of the EU General Data Protection Regulation (GDPR). This policy refers to the above legislation as "the Law."

The requirements apply regardless of whether the data is stored electronically, on paper or in another format.

To comply with the Law, personal data must be collected and used fairly, stored safely and not disclosed unlawfully.

The Law is underpinned by eight important principles. These state that personal data must:

- be prepared fairly and lawfully
- be obtained only for specific, lawful purposes
- be adequate, relevant and not excessive
- be accurate and kept up to date
- not be held for any longer than necessary
- processed in accordance with the rights of data subjects
- be appropriately protected
- not be transferred outside the European Economic Area. Unless that country or territory also ensures an adequate level of protection.

The AHA is registered with the ODPA (Data Commission). Number: DPA4203

2. People, risks and responsibilities

2.1 Data protection policy scope

This policy applies to:

- the AHA
- all employees of the AHA
- all contractors, suppliers or other people working on behalf of the AHA.

It applies to all data that the AHA holds relating to identifiable individuals. This can include:

- names of individuals
- postal addresses
- email addresses
- telephone numbers
- date of birth and age
- tax identification numbers and similar
- health information
- Tax and Social Security information
- any other information relating to individuals.

2.2 Data protection risks

This policy assists in protecting the AHA from data security risks, including:

- **breaches of confidentiality.** For instance, information being provided or given out inappropriately or unnecessarily;
- **failing to offer choice.** For instance, all individuals should be free to choose how the AHA uses data relating to them;
- **reputational damage.** For instance, the company could suffer if hackers successfully gain access to sensitive data.

2.3 Responsibilities

Everyone who works for or with the AHA has responsibility for ensuring that personal data is collected, stored and handled appropriately and in line with this policy and accepted data protection principles.

However, the following have key areas of responsibility:

- The **Board of Directors** of the AHA are ultimately responsible for ensuring that the AHA meets its legal obligations and that there are sufficient resources made available to achieve this
- The **Data Protection Officer** is responsible for:
    - keeping the Board updated about data protection responsibilities, risks and issues.
    - reviewing all data protection procedures and related policies
    - arranging data protection training and advice for employees covered by this policy.

- answering or handling data protection questions from residents, employees or anyone else covered by this policy. Dealing with requests from individuals to see the data that the AHA holds about them, known as Subject Access Requests (see section 7)
- checking and approving any contracts or agreements with third parties that may handle the groups sensitive data

- **Management and the Directors** are responsible for:

  - ensuring all systems, services and equipment used for storing data meet acceptable security standards
  - performing regular checks to ensure security hardware and software is functioning properly
  - evaluating any third-party services that the AHA is considering using to store or process data.
  - approving any data protection statements attached to communications such as emails and letters
  - addressing any data protection queries from the media.
  - working with other employees to ensure that marketing initiatives abide by data protection principles

3. General guidelines

- The only people able to access data covered by this policy should be those who need that data to undertake their daily work as part of the AHA business.
- Data should not be shared informally. When access to confidential information is required, employees should ask management and/or Directors for access
- The AHA will provide training to all employees to assist them in understanding their responsibilities when handling data
- Employees must keep all data secure, by taking sensible precautions and following the guideline below.
- Strong passwords must be used.
- Passwords should never be shared with other employees.
- 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 or inaccurate.
- Data should be deleted and disposed of if it is no longer required.
- Employees should request assistance from management and/or the Data Protection Officer if they are unsure about any aspect of data protection.
- If employees are sending or providing personal data externally outside of the AHA they should always seek approval from the Directors and the Data Protection Officer.

4. Data storage

These rules describe how and where data should be safely stored. Questions about storing data can be directed to the Directors and the Data Protection Officer.

When data is hard stored on paper, it should be kept in a secure place where unauthorised people cannot access or see it.

These guidelines also apply to data that is usually stored electronically but has been printed as a hard copy for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure that paper and printouts containing personal data are not left where unauthorised people could see them.
- When no longer required hard, paper copies should be shredded and disposed of securely.

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 (CD, DVD Memory Stick) these should be kept locked 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.
- Data should be backed up frequently.
- All servers and computers containing data should be protected by approved security software and a firewall.

5. Data use

Personal data is of no use to the AHA 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:

- When working with personal data, employees should ensure their computer screens are cleared and locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email.
- Data must be encrypted before being transferred electronically.
- Personal data should not be transferred outside the European Economic Area without authority and after the recipient jurisdictions data protection laws and policies have been assessed. (Note in their agreements all clients do give permission for data to be transferred inside and outside the European Economic Area)
- Employees should not save copies of personal data to their own computers.

6. Data accuracy

The Law requires AHA to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees to take reasonable steps to ensure data is kept accurate and as up to date as possible.

- Data will be held in as few places as necessary. Employees should not create any unnecessary additional data files.

- Employees should take every opportunity to ensure that data is accurate and updated.
- Data should be updated as inaccuracies are discovered.

7. Subject access requests

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

- ask what information the AHA holds about them and why.
- ask how to gain access to the data.
- be informed about how to keep the data up to date.
- be informed about how the AHA is meeting its data protection obligations.

If an individual contacts the AHA requesting information, this is called a Subject Access Request.

Subject access requests from individuals should be made by email or post, addressed to the Data Protection Officer.

Individuals can be charged £10 for subject access requests. The Data Protection Officer must provide the data within 14 days.

The Data Protection Officer must verify the identity of anyone making a subject access request before sending out any data or information.

8. Disclosing data for other reasons

In certain circumstances, the data protection law allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances the AHA will disclose the requested data. However the Data Protection Officer must ensure that the request is legitimate, seeking assistance from the Board and from the AHA's legal advisers if necessary.

9. Providing information

The AHA aims to ensure that individuals are aware that their data is being processed and that they understand:

- how the data is being used
- how to exercise their rights

To these ends the AHA has a privacy notice, setting out how data relating to individuals, who are residents or employees, is used by the AHA.

In addition employees are informed as to how their data, held by the AHA, is used by the AHA.