ELIM HOUSING GROUP

DATA PROTECTION POLICY

JUNE 2021

1. Introduction

1.1. The UK General Data Protection Regulation (GDPR) became effective in the UK from 31st January 2020. Its purpose is to protect the 'rights and freedoms' of living individuals and to ensure that personal data is not processed without their knowledge and is processed with their consent.

1.2. The GDPR has been accepted as Data Protection (DP) law in the UK with some extensions, as laid down in the UK Data Protection Act, 2018. All DP legislation in the UK is regulated by a supervisory authority called the Information Commissioners Office (ICO). The Elim Housing Group (Elim) is a Data Controller registered with the ICO (reg. no. Z7302750).

1.3. As well as personal data, Elim staff will, on occasions, handle business sensitive data.

1.4. This Policy applies to all of Elim's personal data processing activities in relation to any data subject, including:

- Customers (applicants and residents, whether renting or purchasing property)
- Clients (any organisation, individual or group of individuals receiving a service provided by Elim)
- Suppliers and partners (contractors, local authorities and stakeholders)
- Employees, volunteers and board members.

1.5. The Policy applies to the whole Elim Housing Group, consisting of Elim Housing Association and its profit making subsidiary, Lime Property Ventures.

1.6. The Policy, along with any associated procedures or governance documents will be adhered to by all Elim staff, volunteers and Board Members.

2. Definitions

2.1. Elim recognises **personal data** as any information that relates to an identified or identifiable living individual. This may include:

- Names
- Dates of birth
- Address
- Contact information, such as telephone numbers or emails
- Your image
- Your National Insurance number

2.2. **Sensitive personal data** (formally known as 'special category data') are special categories of data that are subject to additional protections in how they can be gathered and used. Sensitive personal data includes information relating to a person's:

- Ethnic or racial origins
- Political opinions or trade union membership
- Finances
- Sex life
- Philosophical or religious beliefs

2.3. **Business sensitive information** is information that is protected from unwarranted disclosure for legal or ethical reasons, or reasons pertaining to personal privacy or proprietary considerations. It may include:

- Organisational bank details
- Contractual information

In many cases, the appropriate handling of business sensitive information will be proscribed within contracts or documentation related to the information in question.

2.4. **Data Processing** 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. Objectives and Scope

3.1. Elim's residents, service users, staff and partners expect Elim to handle their personal data lawfully, with care and with respect. This policy will outline Elim's approach to the protection of personal data in light of current DP legislation. We are committed to ensuring that we comply with the six data protection principles outlined in the GDPR:

1. Personal data must be processed lawfully, fairly and transparently.
2. Personal data can only be collected for specified, explicit and legitimate purposes.
3. Personal data must be adequate, relevant and limited to the purpose for which the data is processed.
4. Personal data must be accurate and kept up to date.
5. Personal data must be kept in a form such that the data subject can be identified for only as long as is necessary for the processing purposes.
6. Personal data must be processed in a manner that ensures appropriate security.

3.2. In adhering to these principles, we will also ensure that we respect the rights of data subjects regarding data processing and the information that is stored about them:

- The right to make subject access requests regarding the nature of information held and to whom it has been disclosed.
- The right to know how we are using data and under what grounds.
- The right to prevent processing for the purpose of direct marketing.
- The right to be informed about the mechanics of any automated decision making processes that sill significantly affect them.
- The right not to have significant decisions that will affect them taken solely by automated processes.
- The right to sue for compensation if they suffer damage by any contravention of DP legislation.
- The right to request the ICO to assess whether DP legislation has been breached.
- The right to have personal data provided to them in a structured, commonly used and machine-readable format and the right, in certain circumstances, to have that data transmitted to another controller.
- The right to object to any automated profiling that is occurring without consent.
- The right to take action to rectify, block, erase or destroy inaccurate personal data.
- The right, in certain circumstances, to be forgotten.

3.3. Elim's will only process data under at least one of the following grounds:

- The data subject has consented to the processing.
- Processing is necessary to fulfil a contract the data subject has entered into.
- There is a legal obligation to process the data.
- Processing is necessary to protect the data subject's vital interests.

- Where processing is necessary for the performance of a task carried out in the public interests.
- The processing is necessary for the purposes of Elim's legitimate interests (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).

4. **Related Documents**

4.1. Further information about our DP practise can be found in additional organisational documents. These are available either through the web links below or by request from our Head Office. For staff, the documents can all be located at P:\Policies and procedures\Data Protection.

Document	Purpose
Privacy Statement	Provides information to customers about how we operate as a Data Controller, including what personal data we gather and what we do with it.
Subject Access Request Procedure	Outlines the process for customers and staff to follow when making a Subject Access Request.
Data Protection Impact Assessment	A template and guidance we use to assess DP-related risks in a specific activity or project.
Retention Policy and Schedule	Explains how long we retain (store) certain types of personal data for.
Supplier Data Protection Agreement	This is the agreement that we ask our suppliers or sub-contractors to sign to confirm their compliance with our DP policy and principles.
Data Protection: Staff Guidelines	This document provides guidance to staff, helping them to observe DP best practise in carrying out their day to day work.
Data Map	Elim's Data Map details the flow of personal data through the organisation: where it comes from, where it is stored, how it is processed.
Data Breach Procedure	Provides guidance for staff in the event of a data breach.

5. **Individual Responsibilities**

5.1. Whilst all Elim staff are responsible for adherence to this Policy and related documents, certain roles within the organisation have specific responsibilities. These are detailed below. The Elim board have full accountability for Elim's approach to data protection and its performance in this area.

5.2. Data Protection Officer

- Ensure that policies and procedures are up to date and communicated effectively to staff.
- Support good practice among staff and managers
- Provide DP advice and support to the whole staff team.
- Alert the ICO in the event of a suspected breach of DP legislation.
- Act as first port of call for subject access requests.
- Identify training needs for the broader staff team and arrange training in conjunction with HR.

- To provide information, assurance and guidance to the Elim board and Senior Leadership Team in relation to DP as required.

5.3. IT & Digital Manager

- To ensure that Elim's IT and Digital systems provide appropriate Data Security.

5.4. Managers and Team Leaders

- Ensure that collection and processing of personal data within their teams complies adheres to this Policy and associated documents.
- Raise training needs identified to the DPO
- Escalate any specific DP queries to the DPO when specialist advice is required.

5.5. All staff

- Observe good DP practise, as outlined in the Data Protection: Staff Guidelines
- Raise any DP related training needs with their line manager
- Raise any DP related concerns with the DPO or their line manager.

5.6. A failure to observe this policy may lead to formal action under the Disciplinary or Performance Improvement policies and procedures.

6. Access to data

6.1. Staff will only have access to sensitive data that they require in order to fulfil their responsibilities. Access to sensitive data will be managed through various means, including but not restricted to:

- Restricted access to digital files
- Password protection
- Read-only protection
- Physical security measures, e.g. specified keyholders

6.2. Where a member of staff has a concern in relation to a matter of access, this should be addressed as a breach; see 8, below.

7. Training

The Group will provide appropriate training to all employees who use personal data at work. The training will ensure that they understand their data protection obligations and raise staff awareness of their data protection rights and obligations.

8. Response to Breaches

The Group will respond appropriately to any breaches of security of personal and sensitive data. Details of how we will respond to data breaches can be found in the Data Breach Response Procedure.

9. Risk Management and Governance

Data-related risks will be detailed on Elim's organisational Risk Register. The DPO will be the operational owner of these risks. The Finance, Risk and Audit Board Committee will be the corporate owner and will also have responsibility for approval of this Policy.

Dave Peregrine
Head of Operations
June 2021