| | |
|---|---|
| **Policy title** | **Data Protection Policy** |
| **Summary** | This Policy sets out how MSV Housing will fulfill its obligations under the UK General Data Protection Regulations (UK GDPR) and Data Protection Act (2018). |
| **Scope** | The policy applies to all employees and board/committee members. |
| **Author & Job Role** | Sian Leighton, Director - Strategy & Inclusive Culture |
| **Directorate** | Chief Executive's Team |
| **Document Status** | Finalised |
| **Document Reference** | CEX/SE/PO/1.0 |
| **Dates:**<br>- **Draft**<br>- **Approved**<br>- **Ratified**<br>- **Effective from**<br>- **Review by** | <br>November 2022<br>December 2023<br>January 2023<br>January 2023<br>Dec 23 (no changes)/ Dec 24 (no changes – await full review in 25 by Head of Risk & Assurance) |
| | |
| **Impact Assessments:**<br>**Date EIA completed**<br>**Date other IAs completed** | <br>November 2022<br>n/a |
| **Consultation** | Information Governance Strategic Group & External DPO |

**If you are reading a printed version of this document, you should check the intranet to ensure you have the most up to date version.**

## Contents Page

## 1 Introduction & Policy Purpose

In carrying out its day-to-day business and duties MSV Housing ("the Group") needs to collect and use certain information about individuals. This can include customers, employees, board members, suppliers, business contacts and other third parties the Group has a relationship with.

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) place various duties and responsibilities on the Group when processing information. The UK GDPR and DPA also create legal rights for individuals in respect of personal information held and processed.

The purpose of this policy is to:

- set out MSV's overarching approach to ensuring compliance with the data protection legislation and regulations.
- provide information to employees on their obligations in relation to data protection.
- outline the rights of data subjects in relation to personal data.

## 2 Scope

This policy applies to all parts of MSV and to all personal data held and processed by the Group, or on behalf of the Group. This includes data held in any system or format, whether electronic or hard copy and whether it relates to potential, present or past data subjects.

It applies to all employees, temporary workers, consultants, contractors, volunteers and any other third parties who have access to personal data. They must be aware of and are required to comply with this data protection policy and associated procedures. This policy also applies where MSV is a joint controller or where its acts as a processor for another controller.

## 3. Key Legal Requirements

The UK GDPR outlines six principles of data processing, specific legal bases for processing personal data and special categories of personal data as well as specific rights for data subjects and certain exemptions.

Anyone processing personal data on MSV Housing's behalf is expected to comply with these requirements which are summarised below:

a) <u>Principles:</u>

The Group will:

- process personal data in a lawful, fair and transparent manner ('*lawfulness, fairness and transparency*');

- only process personal data for specific, explicit and legitimate purposes, which it will document ('*purpose limitation*');

- only process data that is adequate, relevant and limited to what is necessary for the purposes for which they are processed ('*minimisation*');

- ensure all data processed is accurate and up-to-date to the best of its ability('*accuracy*');

- not keep personal data for longer than it is necessary for the purposes for which it is processed ('*storage limitation/retention'*);

- process data in a secure manner ensuring protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using appropriate technological or organisational measures ('*integrity and confidentiality/security*').

b) Specific Legal Rights

Before any processing activity takes place, MSV Housing will establish the appropriate lawful basis for such processing, which must be one of the following:

- The Data Subject has given consent to the processing of their data: or

- The processing is necessary for a contract the Data Subject is party to, or in order to take steps prior to entering into a contract (e.g. a Tenancy Agreement, or applying for a tenancy); or

- The processing is necessary for compliance with a legal obligation to which the Group is subject, or

- The processing is necessary to protect the vital interests (life) of the data subject or another natural person (e.g. in an emergency life and death situation, disclosing an employee's allergies); or

- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

- The processing is necessary for the purposes of a legitimate interest of the Data Controller or by a third party except where such interests are overridden by the interests or rights and freedoms of the Data Subject, in particular where the Data Subject is a child.

*c)* Rights for data subjects:

The Group will ensure it complies with the following rights:

- *The right to be informed* about the processing of their personal data
- *The right to access* a copy of their data (Subject Access Request)
- *The right to rectification* of their data if it in incorrect;
- *The right to erasure* (also known as 'the right to be forgotten')
- *The right to the restriction of processing*
- *The right to data portability* to allow individuals to obtain and reuse their personal data for their own purposes across different services
- *The right to object* to processing in certain circumstances
- *Rights in relation to automated decision making and profiling*; where the automated decision could have a significant impact on them, and the associated right to request that a human reviews the decision made electronically.

d) Sharing Personal Data

Any data sharing and disclosure the Group undertakes will comply with our legal obligations and follow MSV's procedures to ensure the appropriate checks and verification is carried out.

When we engage in regular sharing arrangements with a third party, we will ensure that both parties sign an Information Sharing Agreement.

e) Transferring Personal Data outside of the UK

Wherever possible, all data processed on behalf of the Group, will be held and managed withing the UK. If, due to certain circumstances data has to be processed outside of the UK then MSV will ensure compliance the relevant requirements of the legislation.

f) Exemptions

There are certain exemptions within the UK GDPR which mean that in very special circumstances MSV does not have to comply with the principles, or with the data subjects' rights. These exemptions include, but are not restricted to:

- Prevention, detection or prosecution of criminal offences
- Taxation, public health or social security purposes
- Protection of judicial independence and judicial proceedings
- Matters of public security, national security or defence
- Safeguarding of children or individuals at risk.

The Group has a number of procedures in place which set out how it complies with the legal requirements covered within this section. These are listed on the Heart under the GDPR section or available from DataProtection@msvhousing.co.uk

## 4 Definitions

| Data Protection Terms | Definition |
|---|---|
| Personal Data | Any information relating to a living, identified, or identifiable individual, e.g., on a computer, CCTV, backed up files, videos, emails, information on telephone logging systems, photographs, text/WhatsApp messages.<br><br>An identifiable individual is one who can be identified, directly or indirectly by reference to:<br>• A name, photo, job title, email address.<br>• An identification number like an employee number.<br>• Location data such as a home address or tracing location of a mobile phone.<br>• An online identifier via IP address, internet cookies, social media account. |
| Data Subject | The identified or identifiable individual whose personal data is held or processed.<br><br>For MSV this includes past, present and prospective:<br>• Employees<br>• Board/Committee Members<br>• Customers, Service Users, Leaseholders<br>• Contractors, Partners and agents<br>• Suppliers |
| Special Categories of Personal Data | Personal data which is more sensitive and so needs more protection, including information about an individual's:<br><br>• Racial or ethnic origin.<br>• Political opinions.<br>• Religious or philosophical beliefs.<br>• Trade union membership.<br>• Processing or genetic data.<br>• Biometric data for uniquely identifying an individual.<br>• Data concerning health.<br>• Data concerning an individual's sex life or sexual orientation |
| Data Controller | A person or organisation that determines (either alone or jointly) whose personal data is held or processed and |

| | |
|---|---|
| | determines the purposes and means of the processing of personal data |
| Data Processer | A person or other body, other than the employee of the data controller, who processes personal data on behalf of the data controller. |
| Processing | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual. |
| Personal Data Breach | A breach of security leading to the accidental or unlawful destruction, Loss, alteration unauthorised disclosure of, or access to personal data. |
| Consent | 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, signifies agreement to the processing of personal data relating to him or her. |
| Senior Information Risk Owner (SIRO) | A Nominated senior professional who has responsibility for implementing and managing information governance risks withing the organisation. |

## 5 Roles and Responsibilities

a) Audit & Risk Committee (ARC) is responsible for:

- Obtaining assurances relating to the adequacy and effectiveness of risk, control and governance relating to data protection at MSV.

c) The Assistant Director - Strategy & Engagement, acting as the Senior Information Risk Officer (SIRO) is responsible for:

- Having overall responsibility for information governance and data protection
- Appointing the Data Protection Officer (DPO) and seeking advice from them as appropriate
- Ensuring that our registrations with the ICO are accurate and up-to-date.
- Acting as the key contact for the ICO
- Establishing and overseeing the information governance framework.
- Ensuring compliance with MSV's information governance policies and standards and reviewing these on a regular basis.
- Reporting regularly to the Executive team and Audit & Risk Committee on data protection compliance.
- Arranging data protection training and advice for all staff members and those included in this policy

- Overseeing the Breach and Subject Access Requests (SAR) registers.
- Providing guidance and advice to colleagues on data protection matters.

d) The Assistant Director – ICT is responsible for:

- Ensuring all IT systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly

d) The Data Protection Officer is responsible for:

- Advising MSV about their obligations to comply with UK GDPR and other data protection legislation.
- Advising, monitoring and assessing the Group's compliance with data protection legislation and making recommendations to improve.
- Providing guidance and advice on data protection to board/committee members, employees and other stakeholders.
- Advising on data protection policies and procedures
- Carrying out data protection audits if required.
- Having direct route to CEO or Chair of ARC or Board, if they deem necessary.

e) The Information Governance Steering Group is responsible for:

- Overseeing, monitoring and maintaining the information governance framework to ensure good practice
- Ensuring compliance with MSV's policy and related procedures and reviewing these on a regular basis
- Contributing to the development and improvement of information governance framework
- Identify and manage information governance risks
- Championing and promoting excellent information governance standards
- Providing guidance and advice to colleagues on data protection matters.

f) Leaders are responsible for:

- Ensuring that all colleagues in their teams understand this data protection policy and related procedures
- Ensuring team members complete relevant data protection training
- Assisting with the implementation of the requirements of UK GDPR and compliance
- Developing any policies and procedures with good data protection principles in mind.

- Encouraging the reporting of data protection incidents as part of continuously improving standards of data protection.
- Support their team members with any queries.

g) Employees are responsible for:

- Complying with this data protection policy and related procedures
- Fully understanding their data protection obligations
- Undertaking data protection training
- Reporting any suspected data protection incidents
- Asking for advice or guidance if they are unsure of any data protection practice.
- Checking that any data processing activities they are dealing with comply with MSV's policy and are justified and lawful
- Raising any concerns, notifying any breaches or errors, and reporting anything suspicious or contradictory to this policy or our legal obligations to their line manager or a member of the IGSG.

## 6. Monitoring, Review & Evaluation

The effectiveness of this policy will be monitored by:

- Regular reporting to the Executive Team and ARC
- Regular review by the IGSG and DPO.

## 7. Policy Review

We will review this Policy every three years and upon changes to the Group. More regular reviews will be considered where, for example, there is a need to respond to new legislation / policy guidance. Reviews will consider legislative, performance standard and good practice changes.

## 8. Related Documents

- Records Management Policy
- Retention Policy & Schedule
- Information Security Policy
- Data Breach Procedure
- SAR Procedure
- DPIA Procedures
- Privacy Statements
- ICT related policies
- Social Media Policy
- Business Continuity Strategy

## 9. Version History

| Version | Date | Description/Summary | Status | Author |
|---|---|---|---|---|
| 0.1 | 11/22 | First draft | Draft | HSE |