Community Counts

Milnbank

Housing Association

53 Ballindalloch Drive, Glasgow G31 3DQ

GDPR –

PRIVACY POLICY

1. INTRODUCTION

Milnbank Housing Association (MHA) is committed to ensuring the secure and safe management of data held by the Association in relation to customers, staff and other individuals. MHA's staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined in this policy and accompanying documentation.

MHA needs to gather and use certain information about individuals. These can include customers (tenants, factored owners etc.), employees and other individuals that MHA has a relationship with. MHA manages a significant amount of data, from a variety of sources. This data contains Personal Data and
Sensitive Personal Data (known as Special Categories of Personal Data under the UK GDPR). This Policy sets out MHA's duties in processing that data, and the purpose of this Policy is to set out the procedures for the management of such data.

2. LEGISLATION

It is a legal requirement that MHA must collect, handle and store personal information in accordance with the relevant legislation, which is:

(a) UK GDPR (as defined by section 3(10) of the Data Protection Act 2018 ("UK GDPR")
(b) the General Data Protection Regulation (EU) 2016/679 ("the GDPR") (insofar as it applies to MHA).
(c) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
(d) The Data Protection Act 2018 (the 2018 Act)

3. DATA

3.1 MHA holds a variety of Data relating to individuals, including customers and employees (also referred to as Data Subjects) Data which can identify Data Subjects is known as Personal Data. The Personal Data held and processed by MHA is detailed within the Fair Processing Notice, the Data Protection Addendum and, for employees, the Terms of and Conditions of Employment.

3.1.1 "Personal Data" is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by MHA and which relates to that individual.

3.1.2 MHA also holds Personal Data that is sensitive in nature (i.e. which includes information that relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is "Special Category Personal Data" or "Sensitive Personal Data".

4. PROCESSING OF PERSONAL DATA

4.1 MHA is permitted to process the Personal Data of data subjects provided it is doing so on one of the following grounds:

- Processing with the consent of the data subject (see clause 3).
- Processing is necessary for the performance of a contract between MHA and the data subject or for entering a contract with the data subject.

- Processing is necessary for MHA's compliance with a legal obligation.
- Processing is necessary to protect the vital interests of the data subject or another person; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of MHA's official authority.
- Processing is necessary for the purposes of legitimate interests.

4.2 **Fair Processing Notice (FPN)**

MHA has produced a FPN which it is required to provide to all customers whose Personal data is held by the Association. That FPN is provided to the customer from the outset of processing their Personal Data and they will be advised of the terms of the FPN when it is provided to them. The FPN sets out the Personal Data processed by MHA and the basis for that Processing. This document is provided to all of MHA's customers at the outset of processing their data.

4.3 **Employees**

Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by MHA. Details of the data held, and processing of that data is contained within the
Employee Fair Processing Notice which is provided to prospective Employees at application stage. A copy of any employee's Personal Data held by MHA is available upon request by that employee from the Association's Data Protection Officer.

4.4 **Consent**

Consent as a ground of processing will require to be used from time to time by MHA when processing Personal Data. It should be used by MHA where no other alternative ground for processing is available. If MHA requires to obtain consent to process a data subject's Personal Data, it shall obtain that consent in writing. The consent provided by the Data Subject must be freely given and the Data Subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained by MHA must be for a specific and defined purpose (i.e. general consent cannot be sought). Where consent is being relied on, Data Subjects are free to withhold their consent or withdraw it at any future time.

4.5 **Processing of Special Category Personal Data or Sensitive Personal Data**

If MHA processes Special Category Personal Data or Sensitive Personal Data, the Association must rely on an additional ground for processing in accordance with one of the special category grounds. These include, but are not restricted to, the following:

- The data subject has given explicit consent to the processing of this data for a specified purpose.
- Processing is necessary for carrying out obligations or exercising rights related to employment, social security or social protection law.
- Processing is necessary for health or social care.
- Processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person.
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest under law.

All the grounds for processing sensitive personal data are set out in Article 9 (2) of the GDPR and expanded on in the Data Protection Act 2018.

5. DATA SHARING

MHA shares its Data with various third parties for numerous reasons in order that its day-to-day activities are carried out in accordance with the Association's relevant policies and procedures. In order that MHA can monitor compliance by these third parties with Data Protection laws, the Association may require the third-party organisations to enter in to an Agreement with MHA governing the processing of data, security measures to be implemented and responsibility for breaches. This will apply in situations where the third party is a joint controller. MHA may also enter into data sharing agreements with other independent controllers where MHA transfers data to those organisations.

5.1 Data Sharing

a. Personal Data is from time to time shared amongst MHA and third parties who require to process the same Personal Data as the Association. Whilst the Association and third parties may jointly determine the purposes and means of processing both MHA and the third party will be processing that data in their individual capacities as data controllers.

b. Where MHA transfers personal data to a third-party organisation which acts as an independent controller (e.g. for administering of the employees' pension), it shall require the third-party organisation to enter into a Data Sharing Agreement with the Association.

5.2 Data Processors

A Data Processor is a third-party entity that processes Personal Data on behalf of MHA and are frequently engaged if certain areas of the
Association's work is outsourced (e.g. maintenance and repair works).

a. A data processor must comply with Data Protection laws. MHA's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify MHA if a data breach is suffered.

b. If a data processor wishes to sub-contact their processing, prior written consent of MHA must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

c. Where MHA contracts with a third party to process personal data held by the Association, it shall require the third party to enter into a Data Processing Agreement with MHA.

6. DATA STORAGE and SECURITY

All Personal Data held by MHA must be stored securely, whether electronically or in hard copy format.

6.1 Paper Storage

If Personal Data is stored on paper, it should be kept in a secure place where unauthorised personnel cannot access it. Employees should ensure that no

Personal Data is left in a place where unauthorised personnel can access it. When the Personal Data is no longer required it must be disposed of by the employee to ensure its secure destruction. If the Personal Data requires to be retained on a physical file, then the employee should ensure that it is affixed to the file which is then stored in accordance with MHA's storage provisions.

6.2 **Electronic Storage**

Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be password protected when being sent internally or externally to MHA's data processors or those with whom MHA has entered into a Data Sharing Agreement. If Personal data is stored on removable media, then that removable media must be always encrypted and stored securely when not being used. Personal Data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

7. **BREACHES**

A data breach can occur at any point when handling Personal Data and MHA has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally in accordance with Clause 7.2.

7.1 **Internal Reporting**

MHA takes the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as it becomes known the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the Association's DPO must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s).
- MHA must seek to contain the breach by whichever means available.
- The DPO must consider whether the breach is one which requires to be reported to the ICO and to the Data Subjects affected and, if appropriate, will do so in accordance with this clause 7.
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

7.2 **Reporting to the ICO**

The DPO will require to report any breaches which pose a risk to the rights and freedoms of the Data Subjects who are subject of the breach to the Information Commissioner's Office ("ICO") within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those Data Subjects affected by the breach.

8. **DATA PROTECTION OFFICER ("DPO")**

A DPO has an over-arching responsibility and oversight over compliance by MHA with Data Protection laws. MHA has appointed a DPO. The Association's DPO's details are noted on MHA's website and contained within the Fair Processing Notice.

The DPO will be responsible for:

- monitoring MHA's compliance with Data Protection laws and this Policy.
- co-operating with and serving as MHA's contact for discussions with the ICO

- reporting breaches or suspected breaches to the ICO and data subjects in accordance with Part 7 hereof.

9. DATA SUBJECT RIGHTS

9.1 Certain rights are provided to Data Subjects under the UK GDPR. Data Subjects are entitled to view the personal data held about them by MHA, whether in written or electronic form. All Data Subject requests must be responded to within one month of receipt of the request. Where several requests have been made by the same individual or the request made is complex, the time for responding may be extended by a further two months. In such cases, the Data Subject must still be advised of that extension within a month of receipt of the request.

9.2 Data Subjects have a right to request a restriction of processing their data, a right to request erasure of their Personal Data and a right to object to MHA's processing of their data. These rights are notified to MHA's tenants and other customers in the Association's Fair Processing Notice. Such rights are subject to qualification and are not absolute.

9.3 Subject Access Requests

Data Subjects are permitted to view their Personal Data held by MHA upon making a request to do so (a Subject Access Request). Upon receipt of a request by a Data Subject, MHA must respond to the Subject Access Request within one month from the day after the date of receipt of the request. The Association:

- must provide the Data Subject with an electronic or hard copy of the Personal Data requested, unless any exemption to the provision of that data applies in law.
- where the Personal Data comprises data relating to other data subjects, must remove or redact that data or, where that is not possible, take reasonable steps to obtain consent from those Data Subjects to the disclosure of that personal data to the Data Subject who has made the Subject Access Request, and, in the absence of consent, consider whether it is reasonable in all the circumstances to disclose that data without consent or
- where MHA does not hold the Personal Data sought by the Data Subject, must confirm that it does not hold any of that Personal Data sought to the Data Subject as soon as practicably possible, and in any event, not later than one month from the day after the date on which the request was made.

9.4 The Right to Erasure

A Data Subject can exercise their right to erasure (otherwise known as the right to be forgotten) by submitting a request to MHA seeking that the Association erase the Data Subject's Personal Data in its entirety.

Each request received by MHA will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO has the responsibility for accepting or refusing the Data Subject's request and will respond in writing to the request. Requests for Erasure will be considered and responded to by the Association by one month from the day after the date we receive the request.

9.5 **The Right to Restrict or Object to Processing**

A data subject may request that MHA restrict its processing of the data subject's Personal Data, or object to the processing of that data. If any direct marketing is undertaken from time to time by MHA, a data subject has an absolute right to object to processing of this nature by the Association, and if MHA receives a written request to cease processing for this purpose, then it must do so immediately.

Each request received by MHA will be considered on its own merits and legal advice will be obtained in relation to such requests from time to time. The DPO has the responsibility for accepting or refusing the data subject's request and will respond in writing to the request.

9.6 **The Right to Rectification**

A Data Subject may request MHA to have inaccurate Personal Data rectified. If appropriate, a Data Subject may also request the Association to have incomplete Personal Data completed.

Each request received by MHA will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the Data Subject's request and will respond in writing to the request.

10. DATA PROTECTION IMPACT ASSESSMENTS ("DPIAs")

These are a means of assisting MHA in identifying and reducing the risks that our operations have on personal privacy of Data Subjects. The Association shall:

- Carry out a DPIA before undertaking a project or processing activity which poses a "high risk" to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data.

- In carrying out a DPIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the Personal Data.

- MHA will consult the ICO if a DPIA identifies a high level of risk which cannot be reduced or mitigated. The DPO will be responsible for such reporting, and where a high level of risk is identified by those carrying out the DPIA they require to notify the DPO within five (5) working days.

11. ARCHIVING, RETENTION AND DESTRUCTION OF DATA

MHA cannot store and retain Personal Data indefinitely. It must ensure that Personal Data is only retained for the period necessary. MHA shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified within Appendix 2 of the UK GDPR Policy.