Printed paper copies of this policy are uncontrolled. The current version of this policy is available on the Portal.

Documentation Master Sheet
Amendments to this document are detailed below

Version Number	Date Amended	Comments	Date Approved	Author	Approved By
1			21/11/18	S Martin	Board
2	3/12/18	Added in location tracking data		S Martin	TB
3	24/9/19	Scope to include subsidiaries and policy ref number amended		S Martin	TB
4	23/12/2021	Review due, changes to legislation only		S Martin	

Policy Number	DP01
Next review due	December 2024
Policy Owner	Data Protection Officer

Related Documents

This policy relates to the following documents:

Personal Data Breach Notification Procedure
IT Acceptable Use Contract
Information Security Procedure
Data Retention Procedure
Data Protection Impact Assessment Procedure
Data Subject Access Request Procedure
Image & Sound Recording Procedure
Staff Handbook

Purpose

People have rights associated with the protection of their personal data and its movement within the UK. Being aware of the risks that we create for others and complying with the data protection principles will align with our objective to 'do the right thing'.

We have a duty to protect the rights and freedoms of our residents, employees, board members, and any other person who entrusts their personal data to us.

> *"The risk to the rights and freedoms of natural persons… may result from data processing which could lead to physical, material or non-material damage, in particular: …to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data…".*[1]

There are penalties for controllers or processors who breach those rights, including –

- the right to an effective judicial remedy against the controller or processor, and
- the right to compensation and liability, and
- administrative fines of up to 20million euros, or 4% of annual turnover, whichever is higher, and
- a temporary or definitive limitation, including a ban on processing.

Following the UK's departure from the EU the UK Government enacted equivalent legislation. This policy sets out how we will meet, as a minimum, the requirements of the UK General Data Protection Regulation (GDPR) 2021 and Data Protection Act 2018.

Scope

Personal data that is processed wholly or partly by automated means, and personal data that is (or is intended to be) part of a filing system is within the scope of this policy.

All data processing by employees of Melin and its subsidiaries and Y Prentis, and third-party processors are within the scope of this policy.

[1] EU GDPR 2016 Recital 75

The principles and terms within this document apply to all personal data, and special categories of data, regardless of the format in which it is held.

Personal data that is used for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security is outside the scope of the GDPR and this policy. For the purposes of this policy, personal data in connection with a criminal offence or in order to safeguard a child or an adult at risk will be shared with the relevant safeguarding authorities or the police.

Anonymised data is data from which it is impossible for any individual to be identified. Anonymised data is outside the scope of GDPR and this policy.

Policy Statement and Principles

We will make sure that the confidentiality, integrity and availability of data is maintained and that arrangements are in place to enable data subjects to exercise their rights –

- to access their data (Data Subject Access Procedure)
- to rectification of inaccuracies in their data,
- to ask to be 'forgotten',
- to restrict processing,
- to data portability,
- to object to processing, and
- to object to automated processing and profiling.

Data Processing Principles

Processing of personal data will comply with the six data processing principles:

1. Processing will be lawful, fair and transparent.
2. Personal data will only be processed for the purposes it was obtained (purpose limitation).
3. Personal data will be accurate and up to date.
4. Personal data will be adequate and limited only to what is necessary (data limitation)
5. Personal data will be held only for as long as is necessary (retention).

6. We will put in place proportionate organisational and technical measures to ensure that personal data is kept securely.

We will use privacy notices to tell data subjects how to contact the Controller and the DPO, explain data subjects' rights, and how to make a complaint. Privacy notices will use plain language to explain the means and purpose (legal basis) of how we will process personal data and who it will be shared with. Privacy notices will be provided at the point of data collection. Where data is provided by a third party, we will notify the data subject, using a privacy notice, within 30 days.

Where the lawful basis for processing relies on the data subject's consent, this will be freely given, specific, informed and unambiguous. We will make withdrawing consent as easy as giving consent.

Specific conditions apply to consent given by children. When offering services to children under the age of 13, we will obtain parental consent.

Processing of special categories of personal data is generally prohibited. We will only process special categories of personal data having first received advice from the DPO on whether one of the conditions at Article 9(2) applies:

- The data subject has given explicit consent;
- It is necessary to fulfil the obligations of the controller or of the data subject;
- It is necessary to protect the vital interests (life-saving) of the data subject;
- Processing is carried out by a foundation or not-for-profit membership organisation;
- The personal data is manifestly made public by the data subject;
- The establishment, exercise or defence of legal claims;
- Reasons of public interest in the area of public health;
- Achieving purposes in the public interest.

The UK Data Protection Act 2018 includes additional conditions and safeguards.

Lawfulness

We will only process personal data where there is a lawful basis for doing so. Article 6 (1) of the GDPR identifies these as:

a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) Processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;

c) Processing is necessary for compliance with a legal obligation to which the controller is subject;
d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) 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;
f) Processing is necessary for the purposes of the legitimate interests pursued by the controller…except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject…in particular where the data subject is a child.

Special categories of data

The UK Data Protection Act 2018 provides for monitoring equality of opportunity. It must not be used:

- to discriminate against or in favour of the data subject,
- if it would cause damage or distress, or
- if the data subject withdraws their consent to processing.

Melin will only process special categories of data for monitoring purposes, and only with explicit consent.

Criminal convictions data

The UK Data Protection Act 2018, Part 2, Chapter 2, section 9(4) provides for processing of personal data relating to criminal convictions by organisations in certain circumstances.

Part 1 of Schedule 1 sets out the conditions relating to employment, social security and social protection. This means that Melin may lawfully process criminal convictions data relating to employment and providing housing (which is listed as a social protection intervention described in Article 2(b) of Regulation (EC) 458/2007 of the European Parliament and of the Council of 25 April 2007 on the European system of integrated social protection statistics (ESSPROS)[2].

Where Melin processes data in respect of criminal convictions, the information will be stored securely and with access limited to a small number of key employees.

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32007R0458

Confidentiality

People who share their personal data with us should reasonably expect that their confidentiality will be maintained. It is the responsibility of all staff to recognise the importance of the confidential nature of information held on its employees, residents and applicants for re-housing, and other external customers.

No member of staff should knowingly divulge information to third parties unless it is lawful to do so.

It is the responsibility of all staff to ensure the security of personal information. Staff and resident files should be locked away when not being used, particularly overnight. When taking files out of the office staff should take reasonable precautions to safeguard the files from loss or damage.

When staff are undertaking work out of the office and require access to personal data, whether in paper form or digitally, it is the responsibility of that member of staff to ensure that all data is secure and kept confidential.

Transferring personal data using unencrypted memory sticks, or by emailing to personal accounts is not permitted and could lead to criminal proceedings by the Information Commissioner.

We will carry out pre-employment checks to establish the trustworthiness of employees handling personal data.

Training

Our employees will have data protection training as part of the induction process and will undertake refresher training at intervals of no longer than 2 years.

Misuse of personal data will be considered as misconduct. Any person found to be operating outside this policy will be dealt with under the Disciplinary and Dismissal Policy. If any breach constitutes an offence under criminal or civil law, court proceedings may be taken.

Data Inventory

We will maintain an inventory of all processing activity.

Data protection by design and by default – Data Protection Impact Assessments (DPIAs)

Our DPIA Procedure sets out the process for initiating a DPIA. A DPIA considers the risks to the data subject. A DPIA is not simply a rubber stamp or a technicality as part of a sign-off process. It's vital to integrate the outcomes of your DPIA back into your project plan. Even if there is no specific indication of likely high risk, we will initiate a DPIA for any new project involving the use of personal data, access to services or involves sensitive data or vulnerable individuals.

The DPO must be involved from the earliest opportunity. We will consult with the ICO prior to processing where the DPIA indicates a high risk to the rights and freedoms of data subjects.

Data retention

Our Data Retention Procedure sets clear guidelines for the retention of personal data and documents, including photographs, CCTV images and voice recordings.

Breach notification

We will comply with the UK General Data Protection Regulations 2021 (GDPR), specifically Articles 33 and 34.

Our Personal Data Breach Notification Procedure sets out our approach to breach detection, investigation and internal reporting procedures. Personal data breaches will be logged on a database. Contracts with Processors will include a clause that they must notify our DPO without undue delay after becoming aware of a personal data breach.

We will notify the ICO of any incident affecting personal data that is likely to result in a risk to the rights and freedoms of data subjects without undue delay and, where feasible, within 72 hours of becoming aware of it.

In accordance with Article 34 we will notify data subjects where the breach is likely to result in a high risk to their rights and freedoms.

Where we are the Processor, we shall notify the relevant Controller without undue delay after becoming aware of a personal data breach.

Data Protection Officer

Our appointment of a DPO is voluntary. Appointing a DPO is mandatory only where –

- Processing is carried out by a public body;
- Core activities require regular and systematic monitoring of data subjects on a large scale; or
- Core activities involve large-scale processing of sensitive personal data or personal data relating to convictions or offences.

Appointing a DPO demonstrates our commitment to privacy and data protection. Voluntary DPOs are subject to all the responsibilities of a mandatory DPO.

The tasks of the DPO are set out in Article 39:

- To inform and advise of obligations;
- To monitor compliance;
- To provide advice with regard to data protection impact assessments DPIAs;
- To monitor performance;
- To co-operate with the supervisory authority (ICO);
- To liaise with the supervisory authority;
- To have due regard to risk associated with processing operations.

Data Subject Access Requests

Except in exceptional circumstances, we will provide, within one month and free of charge, any information or communication referring to the data subject. Instructions are available in our Data Subject Access Requests Procedure and we will maintain a record of all data subject access requests.

Processing card payments

When processing debit and credit card payments we will adhere to the Payment Card Industry Data Security Standard (PCI DSS), which was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.

CCTV, photographs and voice recording

Melin's Image & Sound Recording policy will comply with guidance issued by the ICO. A register of CCTV systems in operation will be maintained.

Photographs are biometric data and can be sensitive data under the GDPR - but only if used for the purpose of "uniquely identifying" someone (Art. 9(1)). Photographs uploaded onto a cloud service would not be considered sensitive data unless used for identification purposes, for instance, using facial recognition systems. When taking photographs at events we will use notices to inform participants that photographs are being taken and how we intend to use them. If we intend to identify the person we will first seek their consent.

Our approach to recording images and sound using CCTV, telephone recording, noise monitoring, and dash cameras in vehicles are set out in the Image and Sound Recording Policy. Requests from data subjects to access their data will be dealt with under Melin's Data Subject Access Request Procedure. Any other request for access to recordings must be documented in the data access log.

Third parties who provide maintenance or editing/redaction services to us will be required to be compliant with data protection regulations.

Information Security Procedure

The confidentiality, integrity and availability of information, in all its forms, are critical to on-going functioning and good governance. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult to recover.

Security failures also creates risks for data subjects, as outlined in the purpose above.

Our Data Security Procedure outlines our approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of our information systems.

We will put in place the necessary technological and organisational measure to protect personal information and achieve Cyber Essentials Plus and IASME accreditation. Given the pace of change in information security, the Data Security Procedure will be reviewed at least annually.

IT acceptable use

Our Data Security Procedure sets out our approach to providing a safe framework for using information technology. Our IT Acceptable Use Policy sets out clear expectations for employees'

use of telephones, mobile phones, storage devices and business applications. This policy will be issued to all new members of staff when attending Data Protection Induction, which will take place on the new employee's first day of employment or as soon as possible thereafter.

Privacy at work

There are laws protecting individuals and laws protecting employers.

- Email – we use email monitoring on the company network. It may take screen snapshots, capture personal passwords, store sent and received emails, identify data exfiltration and block banned websites. The law allows employers to monitor staff email use and is entitled to take disciplinary action for misuse.
- Mobile phones – We receive itemised billing showing numbers called/texted, along with the time, date and duration of call.
- Telephone network – calls are recorded for training and monitoring purposes.
- CCTV – there are systems at our offices and some schemes.
- Information about location obtained through the electronic tracking of company owned vehicles, mobile phones, laptops, tablets and lone worker devices.

Employees must use their discretion to decide if it is appropriate, necessary or important to use business email or telephones for personal business.

There may be situations when it is appropriate for the Technology Team to arrange access to work email or U:drive for another member of staff (usually a line manager), for example when off sick. Before providing access, our Technology Team team will ensure that:

1. The request has been made in writing, says why access is needed, gives enough information to justify the request.
2. Less intrusive alternatives have been considered.
3. The request is entered on a log of requests.
4. Access is limited to the minimum needed, both in terms of the length of time it is available and the extent. Long term access should be reviewed regularly to ensure the ongoing appropriateness.

Contract management

Our processors will be provided with written instructions; agreements with processors will include terms that ensure processors also comply with the GDPR when processing data on our behalf.

Contracts with Processors will include clauses to ensure that processing carried out on our behalf is fully compliant with GDPR. Contracts must set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

Contracts must also include as a minimum the following terms, requiring the processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law.

Contracts with non-IT suppliers will include clauses about data protection and confidentiality where resident or employee personal data is shared.

Record keeping

- Breach notification log
- Data Processing Inventory
- Data Retention Schedule

- Register of CCTV systems
- Data Access Log – image and voice recording requests (not from data subject)
- Systems Register
- Data Subject Access Requests
- Requests for erasure, objections to processing, data portability
- DPIA register
- Data protection training records
- System Penetration Testing results

Performance Standards

Board and Leadership will receive regular reports about data privacy.

Staff training up to date.

Compliance with the 72-hour breach reporting target.

Compliance with the 30-day deadline for responding to data subject access requests.

Contracts with processors will include relevant clauses.

Compliance with the data processing principles.

DPIAs completed.

Equality and Diversity

This policy is in line with the wider Equality and Diversity policy which prohibits discrimination on the grounds of age, gender, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation. We will monitor data subject access requests, breaches of personal data, security testing and DPO monitoring to ensure that we are treating data subjects fairly.

Risks

There is a risk of a loss of data, due to an IT system security breach or Corruption Viruses.

There is a risk of inefficient Hardware and Software or a lack of maintenance support.

There is a risk to the rights and freedoms of data subjects if we fail to implement appropriate organisational and technical measures to comply with the GDPR.

Key Contacts

Data Protection Officer – dpo@melinhomes.co.uk

Technology Team Manager

Responsible Director – Director of Business Improvement

Definitions

Breach - A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. Personal data breaches can include, but are not limited to:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Consent - of the data subject means 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.

Consent declaration – it must be recorded how and when consent was obtained. The declaration may be on a paper or electronic form and must include a data.

Controller – decides what data to collect and how it will be processed.

Data Protection Impact Assessment (DPIA) – A process to identify and reduce the privacy risks of a project or system.

Data subject – an identified, or identifiable person. Often referred to in the regulations as a 'natural person'. A natural person is a living individual.

Filing system – any structured set of personal data which are accessible according to specific criteria.

Personal data – any information relating to an identified, or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as an ID number, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Privacy notices – also referred to as notices of fair processing. They tell the data subject what information will be collected, how it will be processed and who it will be shared with. They demonstrate that data is being processed fairly and transparently.

Processing – includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restructure, erasure or destruction

Processor – a separate natural or legal person which processes personal data on behalf of the controller. Not an employee of the Controller.

Special categories of personal data – race, ethnic origin, political opinions, religion, philosophical beliefs, trade union membership, genetic data, biometric data, health data, concerning a natural person's sex life, sexual orientation. Processing of these types of data is prohibited except in certain circumstances.