OVERARCHING DATA PROTECTION POLICY

Table of Contents

PART 1 – Policy Statement

- Introduction
- Scope
- Related policies
- Roles and responsibilities

PART 2 – Processing Personal Data

- What is personal data?
- When will personal data be processed?
- How personal data must be processed
- What records does UK GDPR cover?

PART 3 – Data Protection Processes and Procedures

- Management responsibility
- Employee and consultant responsibility

PART 4 – Policy Management

- Data protection governance group (DPGG)
- Training
- Monitoring
- Privacy notices
- Individual rights
- Special category data
- Data protection impact assessment (DPIA)
- Retention of records
- Disposal of data

PART 1 – Policy Statement

1. Introduction

1.1 This policy sets out how Keepmoat Limited ("**Keepmoat**") (and its subsidiary companies), complies with its data protection obligations and seeks to protect personal information relating to its customers, employees, temporary and agency workers, contractors, interns, volunteers and apprentices (collectively, "**Staff**"), and sub-contractors.

1.2 The purpose of this policy is to ensure that **Staff** understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their employment. It sets out the roles and responsibilities of each business function and region within Keepmoat, with regard to how **Personal Data** is obtained, stored, used and disclosed.

2. Scope

2.1 This Policy is overarching and applies to all business areas and individuals employed by or engaged by Keepmoat.

2.2 Keepmoat respects the privacy of the **Personal Data** of its Staff, customers and sub-contractors and takes all reasonable steps to ensure that **Personal Data** is processed in accordance with the UK General Data Protection Regulation ("**UK GDPR**") and its **Processing Principles**.

2.3 Keepmoat has implemented various procedures to ensure that all of its business functions and regions comply with UK GDPR. Keepmoat aims to provide its Staff with sufficient training, information and instruction as required for them to identify **Personal Data** and process it appropriately.

2.4 It is the duty of all Keepmoat's **Staff** and the sub-contractors engaged by Keepmoat, to ensure that they are fully aware of this policy and that they comply with its directions in performing their roles. Compliance with UK GDPR is the responsibility of all **Staff** and sub-contractors. Any deliberate breach of this Data Protection Policy and related systems of work and procedures established by Keepmoat to comply with UK GDPR may lead to disciplinary action being taken by Keepmoat, and possibly a criminal prosecution.

3. Related policies

3.1 This Policy applies to all Processing of Personal Data by Keepmoat. It applies in addition to, and is complemented by, the following other policies and procedures:

LEGAL & COMPLIANCE POLICIES	IT POLICIES
Clear Desk policy	Acceptable Use policy
Cookie policy	Bring Your Own Device policy
Data Anonymisation and Deletion policy	Cloud Service Provider policy
Data Subject Access Request policy	Information Security policy
Data Subject Access Request policy - Employees	Privileged Access policy
Data Security Breach Response policy	Technology Disposal policy
Data Retention Principles	
Privacy Notices (general, recruitment, HR)	

4. Roles and responsibilities

4.1 **Executive Board** - has overall responsibility for ensuring this policy complies with Keepmoat's legal obligations and ensuring that all those under Keepmoat's control comply with it.

4.2 **Senior Managers –** have been delegated responsibility for data protection by the Executive Board. For more information, see the Keepmoat Homes UK GDPR Governance and RACI Matrix (reference: **LEG-ST-020**).

4.3 **Data Owners** - have responsibility for ensuring their data is stored and processed in line with the policy and UK GDPR. They must ensure their article 30 records of processing activities (RoPAs) are maintained. See Appendix A for a list of data owners.

4.4 **Compliance Manager** – is responsible for implementing Keepmoat's approach to data protection, providing guidance on the matter, and performing compliance monitoring. The Compliance Manager will co-ordinate responses for individual requesting to exercise their UK GDPR rights.

4.5 **Line Managers** – line managers are responsible for ensuring that their direct reports complete the data protection training assigned to them and process data in line with this policy.

4.6 **All Staff** – are responsible for making sure that they understand this policy, and process data in line with this policy and the Processing Principles set out in UK GDPR.

Data owner responsibilities

4.7 **"Data Owner"** refers to the designated data owners within Keepmoat's business, with data responsibilities as set out in **Appendix A**.

4.8 Each **Data Owner** is responsible for ensuring the following in respect of their business functions and/or region:

- explaining to all relevant Staff the importance of data protection;
- ensuring that all Staff have received adequate training, including (where necessary), information, instruction and supervision to ensure Personal Data is processed in accordance with UK GDPR;
- assuming overall responsibility for compliance with UK GDPR;
- ensuring that data is Processed, retained and destroyed in accordance with this, and the other policies listed in Part 1 and Part 4;
- ensuring that suitable contracts are in place with third parties engaged to process personal data on behalf of Keepmoat ("Data Processors"), including situations where the Data Processor is another company within the Keepmoat group of companies; and
- ensuring that Keepmoat is able to demonstrate how it complies with the requirements of UK GDPR by maintaining an Article 30 statutory record, data sharing maps and system data flow maps (where applicable) of how personal data is kept and processed as set out in **Appendix A**.

Staff responsibilities

4.9 All **Staff** must:

- ensure that they are aware of the issues regarding data protection;

- consider the rights of **Data Subjects** who may be affected by their **Processing** of **Personal Data**;
- **Process Personal Data** in accordance with this policy and any other instructions given to them by Keepmoat from time to time; and
- report receipt of any data subject access requests or other questions regarding data protection or data breaches to the **legal and compliance team** (per the respective policies set out in Part 1).

4.10 **Staff** are responsible for helping Keepmoat keep their personal information up to date. **Staff** should let the **HR Department** know if the information they have provided to Keepmoat changes, for example, if they move to a new house or change the bank or building society account they are paid into. Alternatively, **Staff** can update their own personal information on a secure basis via Keepmoat's intranet.

4.11 **Staff** may have access to the **Personal Data** of other members of staff, customers and subcontractors of Keepmoat in the course of their employment or engagement. If so, Keepmoat expects them to help meet its data protection obligations to those individuals.

4.12 **Staff** should be aware that they may also enjoy the rights set out in the Individual Rights paragraph 4 in Part 2.

4.13 If **Staff** have access to **Personal Data**, they must:

- only access the **Personal Data** that they have authority to access, and only for authorised purposes;
- only allow other **Staff** to access **Personal Data** if they have appropriate authorisation;
- only allow individuals who are not **Staff** to access **Personal Data** if they have specific authority to do so from **the legal and compliance team;**
- keep **Personal Data** secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Keepmoat's **Information Security Policy;**
- not remove **Personal Data**, or devices containing **Personal Data** (or which can be used to access it), from Keepmoat's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
- not store **Personal Data** on local drives or on personal devices that are used for work purposes and comply with the Keepmoat's **Bring Your Own Device Policy.**

4.14 **Staff** should contact the **legal and compliance team** if they are concerned or suspect that one of the following has taken place, is taking place or likely to take place.

- **Processing** of **Personal Data** without a lawful basis for its **Processing** or, in the case of **Special Category Data**, without the condition in paragraph 5.2 of Part 4 being met;
- access to **Personal Data** without the proper authorisation;
- **Personal Data** not kept or deleted securely;
- removal of **Personal Data**, or devices containing **Personal Data** (or which can be used to access it), from Keepmoat's premises without appropriate security measures being in place;
- any other breach of this policy or of any of the **Processing Principles**.

PART 2 - Processing Personal Data

1. What is personal data?

1.1 **"Personal Data"** is data relating to an identified or identifiable living individual. They may be identified:

- from the data; or
- from that data and other information which is in the possession of or is likely to come into the possession of the controller.

It includes obvious identifiers such as name, address, email addresses and contact details but also online identifiers, location data, identification numbers and anything else that could identify someone.

Individuals about whom **Personal Data** is kept are known as **"Data Subjects"**. When Keepmoat holds and uses or processes **personal data** it is called a **"controller"**.

1.2 "**Special Category Data"** is data which relates to the racial or ethical origin of the **Data Subject**, political opinions, religious or philosophical beliefs, trade union memberships, physical or mental health, sexual life or sexual orientation, genetic data or biometric data for the purpose of uniquely identifying a living individual.

2. What counts as processing personal data?

2.1 Keepmoat, its **Staff** and sub-contractors process **Personal Data** when **Personal Data** is recorded, held or used.

2.2 The following activities will constitute the processing of **Personal Data:**

- obtaining, organising, adapting or retrieving data;
- consulting with someone on the content of data or otherwise using it;
- disclosing data by transmitting it, disseminating it or otherwise making it available; and
- combining the data with other data, erasing or destroying it.

3. How must personal data be processed?

3.1 **Personal Data** must be processed in accordance with the **Processing Principles** set out in UK GDPR. In particular it must be:

- processed lawfully, fairly, and in a transparent manner (*Lawfullness, fairness, and transparency)*;
- collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with that purpose (*purpose limitation)*;
- adequate, relevant and limited to what is necessary for the purposes for which it is processed (*data minimisation)*;
- accurate and where necessary kept up to date (*accuracy)*;

- kept in a form that identifies an individual for no longer than necessary for the purposes it was collected (*storage limitation)*
- Processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and loss, destruction or damage (*integrity and confidentiality)*
- Keepmoat are responsible for, and should be able to demonstrate compliance with, these principles (*accountability).*

3.2 Keepmoat, its **Staff** and sub-contractors should assume that whatever they do with **Personal Data** will involve **Processing** it for the purposes of UK GDPR and should therefore only **Process Personal Data**:

- if they have consent to do so; or
- if it is necessary to:
  - fulfil a contractual obligation or as part of the employer/employee or consumer relationship; for example, processing the payroll, or passing customer details to the NHBC;
  - to comply with law;
  - to protect the vital interests of an individual;
  - in the public interest; or
  - in the legitimate interests of Keepmoat or a third party.
  - If you are unsure about whether you can **Process Personal Data** for a particular purpose, please contact the legal and compliance before doing so.

4. Individual rights

4.1 **Data Subjects** (e.g. a customer or employee) have the following rights in relation to their personal information. These rights are enshrined in UK GDPR:

- to be informed about how, why and on what basis that information is processed (*the right to be informed)*.
- to obtain confirmation that their information is being processed and to obtain access to it and certain other information, by making a subject access request—see Keepmoat's Subject Access Request policy and Subject Access Request Policy – Employees (*the right of access)*;
- to have data corrected if it is inaccurate or incomplete (*the right of rectification)*;
- to have data erased if it is no longer necessary for the purpose for which it was originally collected, or if there are no overriding legitimate grounds for the processing (*the right to be forgotten*);
- to restrict the processing of personal information in certain circumstances. This is an alternative to requesting the erasure of their data. Individuals must have a reason for wanting the restriction such as they have issues with the data Keepmoat holds or the way they are processing it (*the right to restrict processing).*

- to receive personal data they have provided to Keepmoat in a structured, commonly used, and machine readable format. Individuals may also request that Keepmoat transmits the data directly to another controller. (*the right to data portability)*

- to object to the processing of their personal data to stop or prevent Keepmoat from processing their data. This can be an absolute right if the data is processed for direct marketing purposes. Otherwise, the request should be assessed on its individual facts (*the right to object).*

- To be informed when automated decision making, including profiling is being used. Individuals can request human intervention of challenge a decision. (*rights related to automated decision making).*

4.2 If a **Data Subject** wishes to exercise any of the rights in paragraph 4.1.2 to 4.1.8, please contact the **legal and compliance team** on GDPR@keepmoat.com.

4.3 **Data Subjects** can request to exercise these rights in writing (eg via letter, email, or a social media post) or verbally.

5. Special category data

5.1 "**Special Category Data**" refers to the information defined in paragraph 1.2 of Part 2 of this Policy.

5.2 Particular care must be taken of **Special Category Data** and all **Staff** who have access to such information shall take particular care to **Process** it properly and in accordance with UK GDPR, the Processing Principles, this Policy and published guidance.

5.3 Employees should make sure that they obtain the explicit consent of an individual before processing **Special Category** Data relating to them. All **Special Category Data** must be stored securely to prevent unauthorised disclosure. This will at least mean storage in locked cabinets and password protection for access to automated data.

5.4 All requests by external bodies, agencies or individuals for access to **Special Category Data** shall be processed by the **legal and compliance team**. All such requests shall be recorded. The record should state the name of the person who made the request, when they made it, what the request was for and to whom it related.

6. What records does UK GDPR cover?

6.1 UK GDPR covers the **Processing** of **Personal Data** either automated processing (e.g. data recorded and accessed by computer in any form) or manual processing (i.e. data recorded in hard copy form) where that is held in a **"filing system"**. A **"filing system"** is a set of information about individuals which is structured by reference to specific criteria:

- by reference to the individual either by name or by an individual's code; or

- by reference to criteria relating to individuals (e.g. age, type of job, holidays);

- such that specific information about an individual is readily accessible.

6.2 This definition is widely drafted and therefore it is difficult to envisage a useful filing system containing information about individuals which would not be covered by UK GDPR.

6.3 You should therefore make sure that all **Personal Data** is processed in accordance with the **Processing Principles.**

PART 3 – Data Protection Processes and Procedures

1. Complaints

1.1 The **Data Owner** must forward any complaints from customers, **Staff,** or any other individual or body to the **legal and compliance team** via GDPR@Keepmoat.com.

1.2 The **legal and compliance team** will be responsible for recording and investigating any complaints to see what improvements can be made to prevent recurrences.

1.3 The **Data Owner** in consultation with the **legal and compliance team** will be responsible for arranging for any improvements to be carried out.

1.4 The record/report should contain the following information:

- the name of the individual making the complaint;
- the date of the complaint;
- the nature of the complaint; and
- the action taken as a result of the complaint.

2. Privacy notices

2.1 Keepmoat will inform customers, **Staff** and prospective **Staff** about the personal information that it collects and holds relating to them, how they can expect their personal information to be used and for what purposes. This information will be set out in our privacy notices:

- For customers – on our website
- For recruitment – on our website
- For employees – on the intranet

2.2 Keepmoat will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

3. Data protection impact assessment (DPIA)

3.1 Where **Processing** is likely to result in a high risk to a **Data Subject's** rights (e.g. where the Company is planning to use a new form of technology), **Data Owner**s will, before commencing the **Processing**, carry out a **DPIA** to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to **Data Subject's** rights; and
- what measures can be put in place to address those risks and protect **Personal Data**.

3.2 Before any new form of technology is introduced, the **Data Owner** should therefore contact the **legal and compliance team** in order that a DPIA can be carried out.

3.3 When conducting any **DPIA**, the **Data Owner** will seek the advice of the **legal and compliance department** and the views of a representative group of employees and any other relevant stakeholders.

3.4 The **DPIA** form can be found in the legal section of the document library.

4. Retention of records

4.1 Keepmoat is required by the UK GDPR to protect and maintain different business data for different periods of time (Retention Periods), and to not keep personal data for longer than is necessary for the purposes for which it was collected and processed (*data minimisation*).

4.2 For more information, Keepmoat's Data Retention & Right to Erasure Principles Policy is published with **Reference: LEG-PO-010.**

5. Data deletion

5.1 Keepmoat is required by the UK GDPR to minimise the data it holds and comply with **Data Subjects'** requests to be forgotten. For more information on the process of data deletion, Keepmoat's policy on Anonymisation and Deletion of Personal Data is published with **Reference: LEG-PO-009.**

PART 4 – Policy management

6. Training and communication

1.1 Keepmoat requires all **Staff** to complete data protection training appropriate to their role. This may include mandatory training and role specific training:

- All **Staff** must complete the data protection e-learning assigned to them.
- **Staff** in roles at high-risk of data protection issues must complete the additional role specific training assigned to them.

1.2 The **legal and compliance team** will conduct a training needs analysis to identify the training each staff group should complete.

1.3 It is the responsibility of the line managers to ensure that all new **Staff** complete training within their first week of employment.

7. Monitoring and review

Monitoring

7.1 This policy will be monitored using the mechanisms listed below:

Requirement	Monitoring	Frequency	Responsible officer
Staff must familiarise themselves with this policy and agree to comply with it.	Staff are required to complete an annual declaration to confirm they have read the policy and agree to comply with it. Completion of declarations will be reviewed.	Annually	Compliance Manager
Staff must complete the data protection training appropriate to their role.	Training records for data protection e-learning are monitored. Levels of compliance included in the monthly compliance report.	Monthly	Compliance Manager
Staff must collect and process data in line with the GDPR Standards agreed for their business area.	Self-assessments against the GDPR Standards will be completed in line with the RACI matrix.	Monthly	Compliance Manager

7.2 all **Staff** who deal with **Personal Data** are expected to be aware of data protection issues and to work towards continuous improvement of the proper **Processing** of **Personal Data** in order to comply with the **Processing Principles**;

7.3 **Staff** who handle **Personal Data** on a regular basis or who **Process Special Category Data** or other **Personal Data** will be more closely monitored;

7.4 spot checks may be carried out by line managers at any time in order to assess any Staff's compliance.

7.5 Employees are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions, and queries should be addressed to the **Compliance Manager.**

Review

7.6 This policy should be reviewed by the owner (Compliance Manager):

- Annually; or
- Upon the change of applicable legislation, regulation, or guidance.

APPENDIX A

Keepmoat Data Owners (approved by the Keepmoat Executive Board)

Keepmoat Data Owners	Data Responsibility
Regional Managing Director supported by Regional Finance Director	All Personal Data (including customer financial data) collected and/or handled by the regional finance team
Regional Managing Director supported by Commercial Director / Regional Head of Commercial	All Personal Data collected and/or handled by the regional commercial team. Maintaining: ▪ Commercial - Article 30 Record for Processing ▪ Commercial (Sole Trader Processing) Data Sharing Map
Regional Managing Director supported by Sales Director / Regional Heads of Sales	All Personal Data (including prospect and customer financial data) collected and/or handled by the regional sales and marketing team (pre-completion) including prospect database, customer journey plot books and customer data in COINS. All marketing campaigns carried out by regional marketing co-ordinators. Maintaining: ▪ Sales - Article 30 Record for Processing ▪ Sales Data Sharing Map
Regional Managing Director supported by Customer Care Director / Regional Head of Customer Care	All Personal Data (including customer financial data) collected and/or handled by the regional customer care team (post-completion) including customer journey plot books and customer data in COINS Maintaining: ▪ Customer Care - Article 30 Record for Processing ▪ Customer Care Data Sharing Map
Regional Managing Director supported by Construction Director / Regional Head of Construction	All Personal Data collected and handled on Keepmoat's sites by the regional construction team Maintaining: ▪ Construction - Article 30 Record for Processing ▪ Construction Data Sharing Map
Chief Financial Officer	All Personal Data (including customer financial data) collected and/or handled by the central finance team Maintaining: ▪ Finance - Article 30 Record for Processing ▪ Finance Data Sharing Map

IT Director	Overall responsibility for Keepmoat's IT systems (including data security, COINS system, HR.net and Miracle Pay system.) Maintaining: ▪ IT - Article 30 Record for Processing ▪ IT Data Sharing Map ▪ COINS System Data Flow Map ▪ HR Data Sharing Map ▪ HR.net System Data Flow Map ▪ Miracle Pay Data Flow Map
IT Director (supported by the Head of Digital Marketing)	Maintaining the prospect database in COINS in accordance with the board approved statement. All marketing campaigns carried out by the central marketing team. Maintaining: ▪ Marketing - Article 30 Record for Processing ▪ Marketing Data Sharing Map
HR Director	All Personal Data collected and stored for the purposes of Keepmoat's HR function. Maintaining: ▪ HR Payroll - Article 30 Record for Processing ▪ HR Talent and Development - Article 30 Record for Processing ▪ HR Administration - Article 30 Record for Processing
HSS Director	All Personal Data collected and stored for the purposes of Keepmoat's HSS function. Overall responsibility for HSS's IT systems including Airsweb system. Maintaining: ▪ HSS - Article 30 Record for Processing ▪ HSS Data Sharing Map
General Counsel and Company Secretary	All Personal Data collected and stored for the purposes of Keepmoat's Company Secretarial function. Overall responsibility for Company Secretary's IT systems including Blueprint system. Maintaining: ▪ Legal - Article 30 Record for Processing ▪ Legal Data Sharing Map