Data Protection Policy

Version Number	2
Revision Date	September 2025
Department	Governance & Transformation
Author	Risk, Governance & Assurance Manager
Reason for Policy Creation/Revision	Planned review as part of the GDPR improvement project
Data Protection	This policy complies with UK Data Protection legislation
Equalities Impact	Not required at this stage
Sustainability Impact	
Proofread By	Head of Governance & Transformation
Date Approved	30 October 2025
Approved By	SMT
Next Review Due	September 2028
Audience – Training and Awareness Approach	This policy will form part of the Good Governance Guide
Effective Date	30 October 2025
Internal References – Policies & Procedures *(Located on HAPI)*	Data Retention Policy Data Protection Procedure FOI/SAR & EIR Procedure Fair Processing Notices ICT Security Policy Data Classification Policy Data Breach Procedure
External References	ICO website UK Government Data (Use and Access) Act 2025: data protection and privacy changes

DATA PROTECTION POLICY

1. Introduction

1.1 This Data Protection Policy applies to all Hanover entities and to everyone who works for or with us. We are committed to meeting our obligations under the UK General Data Protection Regulation (GDPR) whenever we handle personal data relating to our employees, workers, volunteers, contractors, customers (including factored owners, Telecare Customers, Telecare Corporate Customers), website users, suppliers, and anyone else we interact with. This policy demonstrates compliance set out by the Scottish Housing Regulator.

1.2 All employees are expected to read, understand, and follow this Policy and related procedures whenever they process personal data on Hanover's behalf. They must also complete any relevant data protection training provided.

1.3 This Data Protection Policy sets out our key obligations under the UK GDPR and how we will comply with them.

1.4 "Personal Data" means any information or data relating to a living identified or identifiable natural person (Data Subject). This term will include any data that can be used to learn, record or decide something about a Data Subject. The definition of "Personal Data" is very wide, for example, emails may be Personal Data.

1.5 The UK GDPR and this Data Protection Policy apply to all Personal Data which we process regardless of whether that data is stored electronically or hard copy, or whether it relates to past or present employees, workers, customers or supplier contacts, shareholders, website users or any other Data Subjects.

2. Policy Scope

2.1 Hanover is committed to complying with our obligations under the UK GDPR and we recognise that the correct and lawful treatment of Personal Data will maintain confidence in our organisation and will support the provision of successful delivery of our homes and services.

2.2 Compliance with this Data Protection Policy is overseen by our Data Protection Officer (DPO). The Board appoint the DPO on an annual basis. All members of the Executive, Senior and Operational Leadership Teams, and all other Managers are responsible for ensuring that the Hanover employees that report to them:

- Comply with this Data Protection Policy
- Implement this and all related policies and relevant practices, processes, controls and training to ensure such compliance.

2.3 Any questions about the content or operation of this Data Protection Policy or the GDPR, or any concerns that this Data Protection Policy is not being or has not been followed by Hanover employees, please contact the Risk & Governance Team via the data protection mailbox dataprotection@hanover.scot.

3. Commitments

3.1 Hanover will:

- Observe all statutory and common law requirements and uphold expectations of ethical conduct in relation to the use of personal data about customers, employees or otherwise.
- Have particular regard to constraints on the processing of special categories of data in terms of the GDPR.
- Ensure all employees are knowledgeable of the GDPR and are equipped with the knowledge to conduct their daily activities in line with this policy.
- Maintain a current, legally complete, registration with the Information Commissioner's Office (ICO).
- Maintain arrangements for individuals to exercise their rights as outlined in Section 19.
- Identify a post holder to act as Data Protection Officer with responsibility for overseeing and monitoring Hanover's compliance with this policy.
- Report significant policy breaches and remedial actions to the Board in line with the Scheme of Delegation.
- Report data breaches within the required timescales to all necessary parties and keep a record and investigate all breaches.

4. Roles and Responsibilities

4.1 Data protection and security is not one person's job. It is the responsibility of each employee to understand the requirements to maintain a high level of data protection.

4.2 Support is provided via a learning and development training course to offer best practice advice.

4.3 Actual and possible breaches of data protection should be promptly reported to the Risk & Governance Team.

4.4 The DPO, supported by the Risk & Governance team, will be the officer responsible for registering Hanover with the Information Commissioner's Office (ICO) (registration no Z6439206), monitoring procedures and dealing with subject access requests. The registration certificate is located on Hanover's intranet (HAPI).

4.5 All employees handling data are individually responsible for ensuring that they do so in accordance with the law. Particular care should be taken when handling 'special categories' of data. An explanation of this is given at section 6.3 in the policy.

4.6 All employees should ensure that they take care of all personal data they use in the line of their duties. Information should be kept in a secure place and should not be made available to those, both within and outside Hanover, who do not need to see it.

5. Legal Basis of Policy

5.1 It is a legal requirement that Hanover process personal data correctly; Hanover must collect, handle and store personal data in accordance with the relevant legislation.

The relevant legislation to the processing of personal data is:

- The GDPR.
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications).
- The Data Protection Act 2018 (the 2018 Act);

- Data (Use and Access) Act 2025: data protection and privacy changes; and
- Any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the UK General Data Protection, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union.

6. The General Data Protection Regulation (GDPR)

6.1 The GDPR sets out the principles in relation to the processing of personal data. "Processing" encompasses collection, management, disclosure, storage and disposal

6.2 The processing of information covers every action taken in connection with it such as:

- Receiving/collection
- Organising
- Amending and/or altering
- Using
- Disclosing
- Destroying
- Recording
- Storage
- Retrieval
- Consultation
- Dissemination
- Restriction
- Erasure

6.3 Special categories of data, children's data, and data relating to criminal convictions and offences are particularly high risk and therefore are prohibited from processing unless certain conditions are met. The following types of personal data are categorised as "special categories of data":

- Race
- Ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometrics data (where used for identification purposes)
- Health data
- Sex life
- Sexual orientation

6.4 Processing of data relating to criminal convictions and data regarding Children (under the age of 16) also involves greater obligations under GDPR.

6.5 Images, CCTV recordings, and telephone or voicemail recordings all count as personal data. Individuals who may be photographed will be informed that their images could be used in printed materials or on websites, and any requests for image removal should be respected except in limited circumstances. Where Hanover operates CCTV, individuals will be notified that their images may be recorded, and appropriate measures will be taken to ensure data security. Retention periods will depend on the purpose of recording but will be kept to the shortest practicable time, with the Data Protection Officer (DPO) providing advice on a case-by-case basis. Hanover holds no

responsibility for customer-owned CCTV systems, such as Ring doorbells. Similarly, telephone and voicemail recordings may contain information that can identify individuals, either directly or when combined with other data, and will therefore be treated as personal data in accordance with this policy.

6.6 Hanover will maintain a Record of Processing Activities (RoPA) and conduct regular reviews against it to ensure it remains up to date.

7. Lawfulness, Fairness and Transparency

7.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

7.2 The GDPR allows processing for specific purposes, some of which are set out below:

- The Data Subject has given their consent.
- The Processing is necessary for the performance of a contract with the Data Subject.
- To meet our legal obligations
- To protect the Data Subject's vital interests.
- To pursue our legitimate interests (or those of a third-party) for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects.
- The processing is necessary to protect the vital interests of the Data Subject or another person

Hanover will perform this function in full compliance with the UK GDPR and associated data protection legislation, how data is collected, and the specific purpose for processing data is set out within Hanover's Fair Processing Notices.

8. Purpose Limitation

8.1 Personal data will be collected only for specified, explicit and legitimate purposes. It will not be further processed in any manner incompatible with those purposes.

9. Document Retention / Data Minimisation

9.1 Article 5 (e) of the GDPR states that personal data shall be kept for no longer than is necessary for the purposes for which it is being processed. Hanover will keep data in line with our Data Retention Policy available on our website.

9.2 We will ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our Data Retention Policy.

9.3 Information regarding all personal data processed by Hanover will be maintained in the RoPA, which will contain the information stated in Article 30 of the GDPR.

10. Accuracy

10.1 Personal data must be accurate and, where necessary, kept up to date. It will be corrected or deleted without delay when inaccurate.

10.2 We will ensure that the personal data we use, and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. The accuracy of any personal data will be checked at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

11. Storage Limitation

11.1 Some records must be kept for periods specified by law. Hanover will comply with these requirements in order to avoid prosecution or regulatory action. Hanover have a Data Retention Policy which ensures that personal data is deleted after an appropriate time, unless there is good reason to continue to retain it.

12. Security Integrity and Confidentiality

12.1 Personal data will be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

12.2 We will implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. We will exercise particular care in protecting special categories of personal data and criminal convictions data from loss and unauthorised access, use or disclosure.

12.3 Hanover will

- Follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction.
- Maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:
  - **Confidentiality:** only people who have a need to know and are authorised to use personal data can access it.
  - **Integrity:** personal data is accurate and suitable for the purpose for which it is processed; and
  - **Availability:** authorised users are able to access the personal data when they need it for authorised purposes.
  - **Comply with** and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

13. Personal Data Breach

13.1 The GDPR requires us to notify certain personal data breaches to the ICO, and, in certain circumstances, the Data Subject. **All data breaches** will be investigated and recorded internally in line with our Data Breach Procedure.

14. Transfer Limitation

14.1 The GDPR restricts data transfers to countries outside the UK to ensure that a level of data protection afforded to individuals by the GDPR is not undermined. The transfer of personal data originating in one country across borders occurs when employees transmit, send, view or access that data in or to a different country.

14.2 Hanover employees must not transfer personal data outside of the UK unless expressly authorised by both the Data Protection Officer (DPO) and the Head of Digital. Authorisation will only be granted on a case-by-case basis. For example, approval would be required if you were working from a family member's home out with the UK

15. Privacy By Design and Data Protection Impact Assessments (DPIA)

15.1 We must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that process personal data by taking into account the following:

- The cost of implementation.
- The nature, scope, context and purposes of Professing.
- The risks of varying likelihood and severity for rights and freedoms of the Data Subject posed by the Processing.
- Hanover must also conduct a DPIA in respect to high-risk Processing. Details of when we should complete a DPIA and what should be in a DPIA is contained within our DPIA Procedure on HAPI.

15.2 Hanover needs to take privacy seriously when handling personal data. This means they must use the right tools and processes (like hiding or changing personal details to protect privacy) to make sure they follow the rules and keep people's data safe.

16. Sharing Personal Data

16.1 Hanover may share personal data with third parties subject to ensuring certain safeguards and contractual arrangements have been put in place. This could be because of requirements in legislation or due to a common purpose Hanover share with another organisation (for example a common housing register).

Wherever Hanover shares personal data with another organisation the following should be considered:

- Is the sharing of personal data necessary in order to achieve a specified purpose or could the purpose be achieved without sharing personal data? If personal data does not need to be shared, then proceed without sharing the personal data.
- If there is a lawful basis (and where applicable a special condition) for sharing the personal data. For example, where sharing is required by law then a lawful basis will apply. This should be documented.

16.1 **Joint Data Controllers**

When two or more parties collaborate closely and jointly decide why and how personal data should be used, they are considered Joint Data Controllers. They share responsibility for protecting that data and ensuring compliance with data protection laws. An example of this would be A local authority partners with a housing association to deliver a joint tenancy support programme for vulnerable tenants.

16.2 If Hanover is a 'joint data controller' with another organisation – alternatively one of the parties might be the 'data processor' of the other. Depending on the relationship between the parties there may be a legal requirement to put a written agreement in place concerning the use and protection of any shared personal data (or a requirement that our contract contains sufficient data protection clauses)

16.3 Have the Data Subjects been made aware that their personal data might be shared with the relevant organisations for the purpose in question? Fair Processing Notices issued to the relevant Data Subjects should be checked in the first instance,

although it is possible for notification to occur in other ways. Where the Data Subjects have not been made aware then they should be notified accordingly prior to the data being shared.

17. Data Subjects' Rights

17.1 The rights which can be exercised against Hanover by an individual under the GDPR include:

- **The right to be informed**– The right to obtain information about how and why Hanover processes personal data about them.
- **The right to access –** The right to access their own personal data processed by Hanover and obtain a copy of it.
- **The right to rectification** – The right to require Hanover to correct inaccuracies in the personal data held about them and/or to complete any incomplete personal data.
- **The right to erasure ('right to be forgotten')** – The right to require Hanover to erase their personal data in certain circumstances.
- **The right to restriction** – The right to require Hanover to restrict its processing of their personal data, under certain circumstances.
- **The right to data portability** – The right to obtain a copy of their personal data in a certain format, to transmit it to another Controller or to require Hanover to transmit the data directly to the other Controller.
- **The right to object** - The right to object to the processing of their personal data by Hanover under certain circumstances, such as the right to stop processing it for the purposes of direct marketing or the right to object to automated decision making.

17.2 Where Hanover has appointed a Processor (such as a service provider) to process its personal data, Hanover shall retain responsibility for dealing with individual requests relating to that personal data even if the request is received by the Processor and/or relates to personal data held by the Processor. Hanover's standard Data Sharing Agreement and our Terms and Conditions imposes an obligation on the Processor to assist Hanover with responding to individual requests. Where this is in place, this obligation should be enforced where necessary, e.g., to obtain information or copies of personal data from the Processor, or to ask them to delete or to correct it.

Commented [MM1]: I'm wondering if this should be a bullet point in its own right, rather than putting article 21 and 22 of GDPR together, and given the growing use of AI?

Commented [KJ2R1]: Thanks for the comment@Mary Moran We agreed to keep them together for now as Hanover doesn't have any wholly automated decision making algorithms currently in place i.e. we don't have any decisions made by algorithms without any human involvement. The policy will be amended to reflect if that changes in the future.

18. Responding to Data Subject's Rights

18.1 Hanover's Risk and Governance Team is responsible for managing and responding to requests relating to Data Subject's rights and will request support and information from other teams to achieve this in line with the Freedom of Information, Subject Access Request and Environmental Information Request (FOI, SAR and EIR) procedure located on HAPI.

18.2 When a request is received Hanover will log the date on which the request was received so that the request can be actioned within the relevant timescales.

19. Third Parties

19.1 It is possible for third parties (e.g. solicitors, MSPs/MPs, family members etc.) to make requests on Data Subject's behalf.

19.2 Hanover must be satisfied of any third parties' evidence of authority to act on behalf of a Data Subject.

19.3 If the Data Subject has reasonable doubts about a third parties' authority to act Hanover may request evidence.

19.4 The timescales for responding to a request will not begin until such evidence is provided.

20. Timing of Responses to Subject Access Requests (SAR)

20.1 Hanover has a legal obligation to respond to an individual request made under the GDPR, confirming that the request has been actioned without undue delay and in any event within one calendar month of receipt (with the exception of the right to be informed and rights related to automated decision making). In some cases, Hanover may be permitted to extend that time limit for a further two months, taking into account the complexity or a number of requests received from the Data Subject.

20.2 If Hanover believes that it needs to extend the time limit for a response, we will write to the Data Subject within one month of receipt of their request, to inform them of this and give reasons for the delay.

20.3 Note that it may take a significant amount of time to respond to and to action a request and so it is important that a request is promptly identified and dealt with effectively.

20.4 Failure to do so could result in enforcement action from the ICO.

21. Format of Requests

21.1 Requests can be made to any part of Hanover in any form, including verbally, via e-mail, social media or other method. Employees should understand how to recognise requests and who is responsible for dealing with these requests. More details can be found within the Freedom of Information, Subject Access Request and Environmental Information Request (FOI, SAR and EIR) procedure located in HAPI.

22. Responding to Requests

22.1 Hanover has a legal obligation to respond to all requests in a way that is concise, transparent, intelligible and in an easily accessible form, using clear and plain language. Where a data subject has made a request electronically, Hanover will provide its response to the request electronically, where possible, and unless otherwise requested by the data subject.

22.2 Hanover is not permitted to charge a fee for responding to these requests, unless it has clear grounds to assert that a request is significantly unfounded or excessive. Where this is the case, Hanover has the option either to refuse to act on the request or to charge a reasonable fee, taking into account the administrative costs of responding. Any fee charged must be reasonable and reflect Hanover's costs only. Only the Risk and Governance Team will determine this.

22.3 Where necessary (i.e., where there is any doubt as to the identity of the data subject) Hanover will verify the identity of the data subject making the request before actioning it (for example, before providing them with a copy of their data). Where possible, this will be done via Hanover's existing authentication procedures. However, if this is not possible, then Hanover will promptly request additional information to confirm their

identity. The timescales for responding to a request will not begin until the Data Subject's identity has been confirmed.

22.4 A clear audit trail recording any decisions to withhold or provide information in response to a data subject access request or any decision not to comply with the Rights of the Data Subject, will be retained. A copy of the information and data provided to the Data Subject will be retained, together with a copy of any information/data which is not to provided.

22.5 Any requests for data should be made to the Risk and Governance Team via the Data Protection mailbox – dataprotection@hanover.scot who will assist with this matter.

23. Other Controllers of the Personal Data

23.1 Where Hanover is obliged under the GDPR to delete personal data, and where Hanover has made the personal data public or disclosed it to others then, taking account of available technology and the costs involved, Hanover will be required to take reasonable steps, (including technical measures) to inform other Controllers who are processing the personal data, that the data subject has requested the erasure of any links to, or copy or replication of, the personal data.

24. Audit Trail of Refusals

24.1 A clear record of any decisions to erase or refuse a request to erase personal data and to inform/not to inform recipients/request other Controllers to delete personal data, should be retained, including the reasons.

25. Rights related to Automated Decision Making

25.1 The Data Subject has the right to not be subject to Automated Decision Making that have legal or similarly significant effects on data subjects unless certain conditions apply.

25.2 Automated decision-making is when a computer or system makes a decision without any human being involved.

25.3 In such circumstances additional safeguards must be put in place to protect the data subject. The DPO should be consulted if Hanover is considering carrying out any Automated Decision Making.

26. Review

26.1 This policy will be reviewed every 3 years or earlier if required.

Revision History

Version Number	Revision Date	Approval Date	Approved by	Review Reason
1	09/05/2019	09/05/2019		New policy - Updated to reflect new legislation
2	September 2025	30/10/2025	SMT	Reviewed as part of the GDPR improvement action plan
