Data Protection Policy

Version number	2
Date applies from	05/02/2025
Policy owner	Executive Director Governance and Assurance
Next review date	05/02/2028
Strategy link	• Customer focused and equitable services • Safe, well maintained, sustainable and affordable services • Making the most of our resources

Key connected legislation/regulation:

- UK General Data Protection Regulations 2020
- Data Protection Act 2018

Annual Checks

Policy owners should ensure that an annual check of hyperlinks, roles, and names is undertaken. These checks are in addition to formal review process. Please see Policy and Procedure framework guidance for further details.

If you need this information in an alternative language please call

0161 605 7260

For other formats please call

0300 123 5522

Introduction

'ForHousing' will be used throughout this document to refer to all organisations within ForHousing.

ForHousing believes that the proper maintenance, protection and use of personal data is paramount to on-going success and the development of good relationships with its customers, staff, contractors, suppliers and stakeholders.

Scope of Policy

This policy highlights our commitment to protecting personal data that is processed for the purposes of our business. It details how we implement that commitment in regard to the collection and use of personal data. Specifically, how we will:

- Comply with applicable law and good practice.
- Protect the rights and freedoms of individuals whose personal data we process.
- Have appropriate technical and organisational safeguards in place to minimise the risk of a data breach, and to ensure that we act swiftly and effectively to contain the damage caused by any data breach.
- Be open and transparent in the way we collect, use, share, store and delete personal data.

The Data Protection Officer (DPO) for ForHousing is Trish Gorton – Director of Governance and Assurance.

Who Does This Policy Apply To?

The policy applies to all individuals who process personal data on behalf of ForHousing including but not limited to staff, customers, contractors, board members and any affiliated stakeholders.

Data Protection Legal Framework

ForHousing are dedicated to complying with the requirements of the Data Protections Laws in England and Wales. The data protection laws include the UK General Data Protection Regulations 2020 (GDPR) and the Data Protection Act 2018. ForHousing also consider the best practice documents published by the ICO as part of these laws.

The Data Protection Laws apply to personal data which is defined as any information from which a living individual can, or potentially can, be identified, whether by reference to this information alone or when combined with other information (for example a name, identification number, location data, an online identifier or factors specific to the physical, mental, economic, cultural or social identity of a person).

Certain types of personal data are deemed 'sensitive personal data' and are privy to additional protection within Data Protection Law. These special categories are:

Race or Ethnic Origin	Political Opinions
Religious Beliefs	Trade Union Membership
Physical & Mental Health, Biometric Data	Sexuality & Gender

Personal data as covered by the Data Protection Laws can be physical or digital. An organisation that decides the purpose and uses of personal data is a **Data Controller.** ForHousing is a Data Controller, as are those affiliated organisations. This policy shall be read to include these affiliates.

Organisations who process personal data on behalf of or as a service are known as **Data Processors.** Whenever a contractor acts as a Data Processor for ForHousing, an agreement shall be put in place between ForHousing and the Contractor that meets the requirements of Article 28 of the GDPR.

Data Protection Principles

The data protection principles of GDPR form the bedrock of the Data Protection Laws and must be complied with at all times when personal data is processed. The principles that guide our approach to data are outlined below:

1. Used in a way that is lawful, fair and transparent.
2. Only collected for a specified, explicit and legitimate purpose.
3. Adequate, relevant and limited to what is necessary for processing purposes.
4. Accurate and up to date.
5. Kept in a form which allows identification of individuals for no longer than necessary.
6. Kept appropriately safe against unauthorised processing, accidental loss, destruction or damage.

Lawful Conditions for Processing

The first data protection principle only permits data processing if there is a lawful basis for doing so. Article 6 of the UKGDPR outlines the lawful bases:

1. The individual has provided their consent for the use of their data for a particular purpose.
2. The use of an individual's data is necessary for the performance of a contract with the individual.
3. The processing is necessary for compliance with a legal obligation imposed on the Data Controller.
4. The processing is necessary in order to protect the vital interests of the individual or another.
5. The processing is necessary for the performance of a task in the public interest.
6. Processing is necessary for the purposes of legitimate interest of the Data Controller, except where these interests are overridden by the interests or rights of the individual.

ForHousing will only process personal data where we can rely on one of the six legal bases, and/or any other set out in Data Protection Law. Where the processing involves Special Category Data, then we will also be reliant on an additional bases from Article 9 of the GDPR. Guidance is available in the ForHousing Special Category Data Processing Policy.

ForHousing shall keep a Record of Processing Activity (ROPA) which documents the legal bases for each of our processing operations.

ForHousing will make use of Privacy Notices to keep individuals informed of how their personal data is being used.

Consent

Where consent is the lawful basis for processing personal data, the consent must be freely given by the individual. If there is an imbalance of power between us and the individual, consent can rarely be said to be freely given. Typically, there is an imbalance of power between an employer and employee. In most cases making the provision of an individual's consent a condition for us to provide a service to that individual will call into question whether the consent was given freely, so in those cases we should avoid the use of consent if possible.

Consent must also be specific. We need to be clear about what we are seeking consent for, and the request should not exceed what is necessary for meeting the specified business purpose. The individual must also take an active step to indicate that they are providing their consent; silence, pre-ticked boxes or inactivity do not constitute consent.

Consent must be recorded in writing and stored in digital or hard copy format

Consent can be withdrawn at any time, and the method of doing so should be clearly explained both on the consent form and in the appropriate Privacy Notice. Once consent has been withdrawn, we cannot seek to rely on another lawful basis to continue processing the same kind of personal data for the individual who has withdrawn their consent.

Individual's Rights

The Data Protection Laws set proscribe a set of rights that an individual has relating to the use of their personal data. ForHousing will respect those rights and where appropriate, will comply with all requests as swiftly as possible. The processes we follow can be found in:

1. Data Transparency where an individual makes a request under Article 15 of the UKGDPR
2. Subject Access Request Procedure where an individual makes a request under Article 15 of the UKGDPR.
3. Data Erasure Procedure where an individual makes a request under Article 17 of the UKGDPR.

ForHousing will follow the best practice guidance as published by the ICO in respect of:

1. Rectification of personal data (Article 16 UKGDPR).
2. Restriction of processing of personal data (Article 18 UKGDPR).
3. Portability of personal data (Article 20 UKGDPR).
4. Objection to processing (Article 21 UKGDPR).
5. Right to not be subject to Automated Decision Making (Article 22 UKGDPR).

The Data Protection Officer or Business Partner for Data Protection will be notified of all requests as soon as possible, and they will be recorded and actioned in the Data Subject Rights Request Log.

If an individual is not satisfied with our response to a request, then they will be informed of their

right to raise a complaint with the ICO.

Transparency

ForHousing will be clear about how personal data is used. Through the use of Privacy Notices we will make clear:

1. What data we are processing.
2. How the data is used by ForHousing or any Data Processors.
3. Our purposes and legal bases.
4. Who personal data may be shared with.
5. The period for which data will be stored (inside the EEA or elsewhere).

Privacy Notices will be published on the ForHousing website, or where applicable, made available to the relevant parties at the point of data collection. In keeping with Principle 4, the Privacy Notices will be kept up to date, accurate and relevant to the category of individual they address.

ForHousing's commitment to the right of transparency is further elaborated in the Data Transparency and Subject Access Request Procedure.

Data Protection by Design and Default

The Data Protection Laws place obligations on us to consider the data protection implications of any project or process at inception and throughout the life of processing. ForHousing will consider data protection wherever personal data is processed.

Whenever ForHousing engages a data processor to act on our behalf, they will also have to consider data protection by design and default.

The Data Protection Laws outline our responsibilities to records any data processing activities as per Article 30 of the UKGDPR. The Record of Processing Activity (ROPA) shall be developed and maintained by the Data Protection Team and verified by the Data Protection Officer.

Where required, the ROPA will be made available to the ICO or other relevant organisations for inspection and compliance purposes.

ForHousing will also make use of Data Protection Impact Assessments (DPIA) as highlighted in Article 35 of the UKGDPR. The DPIA will be used to assess the impact of processing on an individual and shall be used at the beginning of a new project. Further information about their implementation and use can be found in the DPIA Assessment Procedure and Toolkit.

Data Sharing & Transferring

ForHousing will not share personal data without having a lawful basis for doing so. The ForHousing privacy notices detail with whom personal data may be shared.

Often times consent will be required for personal data to be shared, where this is the case, a copy of the individual's consent will be maintained by the appropriate team. Other types of data sharing may happen without prior notification, such as when data is shared in the prevention or detection of crime. The veracity of any request will be confirmed, and where necessary the

guidance of the DPO will be sought before any personal data is shared.

If sharing is taking place to another organisation as a one-off project, then ForHousing will determine if a Data Sharing Agreement and/or Non-Disclosure Agreement is appropriate. As above, advice from the DPO should be sought prior to a decision being made. If a Data Sharing Agreement is signed, then a copy will be held by the Data Protection Team.

When data is shared, it will be done so through an appropriately secure method, such as an encrypted email or secure portal (after validation from IT).

ForHousing will not share personal data outside of the EEA unless the DPO confirms that the transfer is lawful and appropriate to the circumstance.

Data Risks, Breaches and Security

The ICO defines a data breach as '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.'

ForHousing aims to ensure that it takes all reasonable measures to protect the personal data that it processes and the individuals from serious risk associated with a data breach.

As part of this commitment, ForHousing will:

1. Ensure that all parties processing personal data are properly trained and aware of the degrees of access, as well as the potential risks and mitigations.
2. Promote the importance of data protection and a respect for personal privacy.
3. Where reasonable, take steps to terminate contracts with processors who do not apply sufficient levels of protection when processing personal data.

Whenever a third-party processes personal data on behalf of ForHousing and there is a data breach, suspected or near miss, they must report it to the Data Protection Team as soon as possible. The Data Protection Team will then take the necessary steps to ensure that the incident is resolved.

The Data Protection Team will maintain a Data Breach and Near Miss register in order to record lessons learned
.
Any notifiable breach will be reported by the DPO or Business Partner to the ICO within the 72-hour deadline after having been discovered.

Roles and Responsibilities

Roles and responsibilities are set out within our Data Protection and Data Governance Framework.

Equity, Diversity, and Inclusion

No negative effects were identified during the IDMF process. Positive effects can be realised when service delivery is being delivered in a bespoke and customer centric manner, using data effectively. Impacts and change will be monitored through day-to-day interactions with tenants

that are data driven. The policy will protect tenants and staffs' rights in relation to the handling of personal data.

We value diversity and work to create an inclusive environment for our customers and colleagues, where everyone has access to the same opportunities. We welcome our responsibility to comply with equalities legislation and regulatory requirements that relate to equity, diversity and inclusion and aim to do more. Through our activities we aim to remove systemic barriers to equal opportunities and eliminate all forms of discrimination, harassment, and victimisation within our organisation.

We are committed to providing excellent customer services, which are fair, equitable and inclusive. As such, we will endeavour to understand and make any reasonable adjustments required for customers in line with ForHousing's Reasonable Adjustment Statement and the Equality Act 2010. Any reasonable adjustment provided will be recorded and kept under active review.

Implementation and Communication

The policy will be delivered through the day-to-day roles of all staff who will ensure compliance with data protection legislation in all the work that they carry out.

ForHousing will provide training materials and guidance to staff to ensure consistent application of the policy, including mandatory E-learning and news stories on the intranet when required.

ForHousing will monitor the application of the policy and ensure ongoing monitoring of compliance against this policy.

This policy will be available both on the intranet and ForHousing website.

Monitoring, Recording, Reporting

Breaches and SARs re reported quarterly to the Audit and Risk Committee within the assurance dashboard.

Business Critical Control audits will be completed by our internal auditors annually giving assurance on:

- Data Protection Impact Assessment - Confirming that all major projects / change projects have a completed DPIA.
- Data Breaches - Confirming that all potential data breaches have been investigated in line with Policy requirements, learnings have been documented and where required, reported externally and internally.

Data Protection audits will take place in line with Data Protection Law requirements at regular intervals, but no less than once every three years unless, due to the number/severity of data breach incidents over a 6-month period requires an audit be completed sooner. This will be at the discretion of the DPO and EMT.

Related Documents

The Data Protection and Data Governance Framework lists all relevant documents to this policy.

Co-production

The policy has been reviewed by the Data Governance Group and also the ED&I Excellence Group.

Approval & Review History

With effect from 23/10/2024 the approval route for the Data Protection Policy is:

- EMT - ARC

Date	Version	Approved by	Detail
25.01.2021	1	EMT	First version, previously ForViva Data Protection Policy
18.01.2022	1.1	N/A	Document reviewed no amendments
01.03.2023	1.2	N/A	Change to policy holder.
05/02/25	2	EMT / ARC	(IDMF – 03/12/24 / SLT Review 10/12/24) Overhaul of policy including introduction of chapter of consent, job roles reviewed.