

General Data Protection Regulation (GDPR) Policy

Scope of Policy

This Policy sets out the key principles by which Platform Housing Group will ensure we comply with legal requirements in respect of data protection. The Policy has been updated to take account of the General Data Protection Regulation (GDPR), which is effective from 25 May 2018.

Applicability

The Policy applies to Platform Housing Group Limited and other Group members.

1. Policy Statement

- 1.1 Platform Housing Group recognises that everyone has the right to expect that safeguards will be put in place and maintained to ensure the integrity of any personal information supplied to members of the Group. We will ensure that we comply with all legal and regulatory requirements to fulfil this obligation.
- 1.2 This policy applies to all personal and sensitive personal data processed on the Group's computer systems and stored in relevant filing systems.

2. Context

- 2.1 The Data Protection Act 2018 (The Act) is designed to protect the individual and their personal data, which is held and processed on their behalf. The Act fully encompasses the European Union General Data Protection Regulation (GDPR). This policy takes into account the definitions and principles set out in both the Act and GDPR.

A glossary is listed below to assist with understanding of some of the terminology of the legislation:

Consent

This means consent of the data subject that is freely given, specific, informed and unambiguous indication of the data subject's wishes by which she or he, by a statement or clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data

Any recorded information held by Platform Housing Group and from which a living individual can be identified be this on paper or electronically.

Data Controller

A natural or legal person (in our case Platform Housing Group) registered with the Information Commissioner's Office who determines the purposes and means of the processing of personal data.

Data Processor

A natural or legal person, public authority, agency or any other body that processes personal data on behalf of the Controller. Examples of this would be 3rd party contractors such as Worcestershire Telecare or Cintra Payroll.

Data Protection Officer

The appointed Officer whose role in the Organisation is to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

Data Subject

A living individual who is the subject of the personal data/information. Examples would be current and former tenants and staff.

General Data Protection Regulation

The General Data Protection Regulation forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of this apply, like the GDPR, from 25 May 2018.

Information Commissioner's Office (ICO)

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. They are the Supervisory Authority (SA) for the UK.

Personal Data

Information relating to a living identifiable individual. Examples would include name, address, contact details, IP address plus any other information related to the individual.

Privacy and Electrical Communications Regulations (PECR)

These sit alongside the GDPR and Data Protection Act. They give people specific privacy rights in relation to electronic communications. There are specific rules on marketing calls, emails, texts, faxes and cookies (and similar technologies).

Processing

Any activity/operation performed on personal data - whether held electronically or manually, such as obtaining, recording, holding, disseminating or making available the data, or carrying out any operation on the data. This includes, organising, adapting, amending and processing the data, retrieval, consultation, disclosure, erasure or destruction of the data. It is difficult to envisage any activity which does not amount to processing.

Special Category Data

More sensitive information relating to an individual's race/ethnic origin, political opinions/affiliations, religious beliefs, trade union membership, health related, sexual life and biometrics.

2.2 The Information Commissioner who oversees compliance and promotes good practice, requires all data controllers who process personal data to be responsible for their processing activities and comply with the 7 GDPR principles. The principles are aligned with the rights of Data Subjects and establish the underpinning obligations of Data Processors and Data Controllers.

2.3 Article 5 of the GDPR requires that personal data shall be:

- 1. Processed lawfully, fairly and in a transparent way in relation to individuals.
- 2. Collected for specific, explicit, and authentic purposes.
- 3. Adequate, relevant, and limited to what is needed.
- 4. Accurate and kept up to date.
- 5. Retained only for as long as necessary.
- 6. Processed in an appropriate way to maintain security.

Article 5(2) requires that:

- 7. The Controller shall be responsible for, and be able to demonstrate, compliance with the principles.

2.4 The GDPR details specific conditions to fair and lawful processing. The Group will ensure that at least one of the following conditions are met before we process any personal data:

- Consent of the data subject
- Processing is required for the performance of a contract with the Data Subject or to move towards entering into a contract.
- Processing is required for compliance with a legal obligation.
- Processing is required to safeguard the vital interests of a Data Subject.
- Processing is required for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.
- Necessary for the purposes of legitimate interests pursued by the Controller or a third party, except where such interests are outweighed by the interests, rights or freedoms of the Data Subject.

2.5 Additional conditions must also be satisfied for Special Category Data.

The Group will ensure that one of the following additional conditions are met before we process any special category data:

- The individual has explicitly consented to the processing;
- Processing is required for carrying out obligations under employment, social security or social protection law;
- Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally unable to give consent;
- Processing relates to personal data manifestly made public by the data subject;
- Processing is necessary for the establishment, exercise or defense of legal claims;
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the data subject;
- Processing is necessary for archiving purposes in the public interest.

For certain special categories of personal data (for example race, ethnic origin, religion or belief, health data or sexual orientation), we will in addition process this data for reasons of equality of opportunity or treatment and where processing of the specified category/ies of data is necessary for the purposes of identifying or keeping under review the existence of equality of opportunity or treatment.

- 2.6 Additional procedural security will be put in place for transgender data subjects holding a Gender Recognition Certificate.

Section 22 of the Gender Recognition Act 2004 establishes that it is an offence for a person to disclose information acquired in an official capacity about a person's application for a gender recognition certificate or about the gender history of a successful applicant.

- 2.7 Platform Housing Group will ensure that at all times we comply with the above principles in respect of how we handle personal data.

3. Aims and Objectives

- 3.1 The Group will ensure that each member complies fully with legal requirements to register with the Information Commissioner's Office (ICO), and to notify the ICO the type of personal data each needs to process, the purpose/s this is processed for and who this will be disclosed to.

- 3.2 We recognise that data subjects have the **right to rectification** of inaccurate personal data and will ensure that any such personal data held will be corrected or erased as appropriate, and recognise that data subjects may seek redress for any damage caused as a consequence of this.

- 3.3 The Group recognises that data subjects have the **right to the erasure** of personal data where one of the following grounds applies and will ensure that we comply with this requirement where applicable where this is technically possible:

- The data is no longer necessary in relation to the purposes for which it was originally collected or otherwise processed;
- The data subject withdraws the consent on which the processing is based and where there is no other legal ground for the processing;
- The data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- The personal data has been unlawfully processed;
- The personal data has to be erased for compliance with a legal obligation; or,
- The personal data has been collected in relation to the offer of information society services.

- 3.4 The Group also recognises that data subjects have the **right to restriction of processing** where one of the following circumstances applies:

- The accuracy of the personal data is contested by the data subject;
- The processing is unlawful, and the data subject opposes the erasure of that personal data, and requests the restriction of its use instead;

- The controller no longer needs the personal data for the purposes of the original processing, but the data is required by the data subject for the establishment, exercise or defence of legal claims; or,
- The data subject has objected to processing pending the verification of whether the legitimate grounds of the controller override those of the data subject.

3.5 The Group also recognises that Data subjects have the **right to object** to electronically generated direct marketing, including profiling. Direct marketing means the communication (by whatever means) of any advertising or marketing material which is directed at them. Platform Housing Group has adopted best practice from the Privacy and Electronic Communications (PECR) Regulations.

3.6 **Data Subject Access Requests**

We recognise that individuals have the right to obtain a copy of personal data held about them on computers and in relevant manual filing systems. Any person who wishes to obtain a copy of their personal data should write to the Group's Data Protection Officer. The person seeking this data (known as the Data Subject) may need to provide proof of identity in order for us to reply to their request within the one calendar month legal period permitted. In some complex cases we may also write to the data subject within the initial one month period to request a further extension of two months in order to provide this data.

The Group will review this approach only in relation to requests that are considered to be excessive or vexatious and will explain the reasons for this to the relevant data subjects.

3.7 The **right to data portability** enables data subjects to acquire and re-use their personal data for their own purposes across different services. In the event of any such requests, the data will be provided in a structured, commonly used and machine readable format. The information will be provided for free and within one month of the request being received and verified. We recognise that any requests to exercise this right will be rare and limited and should be made in writing for consideration by the Data Protection Officer.

3.8 **Rights related to Automated Decision Making and Profiling**

Data subjects have the right not to be subject to an agreement when it is focussed on automated processing. Platform Housing Group do not carry out any processing based on automated decision making or profiling at present.

3.9 The **Right To Be Informed** covers the necessity to provide fair processing information. Platform Housing Group shall meet its obligations under this right by ensuring privacy notices are used when any personal data is collected. The privacy notices shall be concise, transparent, understandable and easily accessible. They will also use clear and plain language.

3.10 **Data Privacy Impact Assessments (DPIA)** are a tool that can be used to identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy. They are an integral part of taking a privacy by design approach. Platform Housing Group will carry out a DPIA when using new technologies where the processing is likely to result in a high risk to the rights and freedoms of individuals. The subsequent findings of the DPIA must then be submitted to the Data Protection Officer for review.

3.11 **Sanctions for non-compliance**

There are a number of tools available to the Information Commissioner's Office for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice on a data controller up to the value of 4% of turnover.

3.12 We will appoint a key member of staff as the Group's **Data Protection Officer**.

The Data Protection Officer will:

- Act independently, be adequately resourced and report to the highest management level,
- Ensure that the Policy and Information Governance Framework is documented, up to date, fit for purpose and being followed,
- Ensure adequate provision of training,
- Inform and advise the organisation and its employees of their data protection obligations under the GDPR;
- Monitor the organisation's compliance with the GDPR and internal data protection policies and procedures. This will include monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits;
- Advise on the necessity of data protection impact assessments (DPIAs), the manner of their implementation and outcomes;
- Serve as the contact point to the data protection authorities for all data protection issues, including data breach reporting;
- Serve as the contact point for individuals (data subjects) on privacy matters, including subject access requests.

4. Policy Outline

4.1 Platform Housing Group is fully committed to compliance with the Act and GDPR. It regards the lawful and secure processing of personal information as fundamental to operating efficiently, in a non-discriminatory manner, offering excellent customer services and ensuring the highest confidence by customers in the integrity of our data processing systems.

4.2 We will seek only to access information that is necessary to hold, know or process. All information held will be kept for no longer than is necessary for the purpose required, and will be kept secure at all times. The Group will implement appropriate organisational and technical measures to ensure security of processing

and compliance with this policy and legal requirements. We will also undertake data protection impact assessments where appropriate.

- 4.3 The Group recognises that there are certain special categories of data (e.g. race, ethnic origin, religion, trade union membership, health data or sexual orientation are some examples) for which processing of such data is prohibited in all but a number of specified exceptions and will ensure we comply with this requirement.
- 4.4 We will ensure that all individuals concerned are made aware of the identity of the data controller, the reasons why any personal and sensitive information is required, how it will be processed and stored securely, and the process for disposing of it. We will also advise individuals of the circumstances when we will need their consent to share this information.
- 4.5 In those circumstances where we rely on the consent of the data subject (e.g. other than where consent is not necessary for the performance of a contract) to process their personal data, we will ensure that this has clearly been given, and that this can be easily withdrawn at any time.
- 4.6 Through its Information Asset Register the Group will maintain an up to date record of processing activities undertaken which will contain the following information:
 - The name and contact details as applicable of the controller, any joint controller, controller's representative and Data Protection Officer;
 - The purposes of the processing;
 - A description of the categories of data subjects and the categories of personal data;
 - The categories of recipients to whom the personal data has been or will be disclosed;
 - Any international transfers of personal data and the documentation of appropriate safeguards;
 - The envisaged time limits for erasure of the different categories of data; and,
 - A general description of the technical and organisational security measures implemented.

When obtaining personal data we will provide data subjects with the following information (e.g. through a privacy notice):

- The identity and contact details of the data controller and representative;
- The contact details of the Group's Data Protection Officer;
- The purposes of the processing as well as the legal basis of the processing;
- The legitimate interests pursued by the controller or by a third party;
- The recipients of categories of recipients of the personal data, if any; and,
- Where the data controller intends to transfer the personal data to a third country and the existence of adequacy conditions where relevant.

We will also provide data subjects with the following additional information:

- The period of time the data will be stored (see also Group Data Retention Policy);
- The right to rectification, erasure, restriction or objection as applicable;
- The right to data portability (right to have personal data transmitted to another data controller) where relevant;
- The right to lodge a complaint with a supervisory authority (e.g. the ICO);
- The consequences of the data subject's failure to provide data; and,
- The existence of automated decision-making, including profiling, as well as the anticipated consequences for the data subject.

4.7 We will seek to ensure that a data processing agreement is applied to all contracts and agreements where a member of Platform Housing Group is contracting out the processing of personal data to another party. This agreement will outline the respective roles and responsibilities of the data controller and data processor in such circumstances and include the following requirements of data processors acting on the Group's behalf:

- Process the personal data only on clear documented instructions from the Group as controller;
- Ensure that those authorised to process the personal data observe confidentiality;
- Take appropriate security measures;
- Respect the conditions for engaging any other processor where applicable;
- Assist the controller by implementing appropriate technical and organisational measures;
- Assist the controller in ensuring compliance with the obligations in respect of security of processing;
- Deletes or returns all personal data to the controller after the end of the provision of services;
- Makes available to the controller all information necessary to demonstrate compliance with this policy and related regulations;
- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of Platform Housing Group, are aware of this policy and the Group's responsibilities as Data Controller, and are fully trained in and are aware of their duties and responsibilities under the Act; and,
- Allow data protection audits to be undertaken by or on behalf of Platform Housing Group of data held on its behalf (if requested).

4.8 We will make sure that all tenancy, lease, licence agreements and employment contracts have a statement confirming the Group's approach and requirements in respect of data protection.

4.9 We will follow the Information Commissioner's Codes of Practice where applicable in developing relevant policies and procedures.

- 4.10 We will ensure that all staff are fully trained and aware of this policy and supporting procedures. We may undertake disciplinary proceedings in circumstances where employees fail to adhere to this and related policies/procedures.
- 4.11 A personal data breach refers to a protection breach that results in the loss, destruction, alteration, unauthorised disclosure of, or access to, personal data. All IT and data breaches/incidents should be reported in accordance with corporate IT security policies and immediately notified to the Data Protection Officer who will escalate the issue up to the appropriate GET member. Where a breach is likely to have a significant detrimental effect on individuals, it should be reported to the ICO within 72 hours and to the data subject without undue delay. This reporting should only be undertaken with the explicit authorisation of GET. A record of all data breaches will be maintained, regardless of whether they are reported to the ICO and data subjects.
- 4.12 All managers and staff will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:
- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
 - Personal data held on computers and computer systems is protected by the use of secure passwords; and,
 - Individual passwords should be such that they are not easily compromised.
- 4.13 This policy forms the bedrock of Platform Housing Group's Information Governance Framework (IGF). The IGF consists of relevant policies, procedures, registers, agreements and programmes.

When followed, the IGF will ensure that all employees, board members, panel members, contractors, agents and partners are fully aware of, and abide by, their duties and responsibilities under the GDPR.

- 4.14 The Information Governance Framework provides the Group's evidential base for demonstrating compliance with the Act and GDPR. Monitoring of Standards and KPIs is undertaken quarterly by the GDPR Forum with updates being reported also to GET. Board will receive an annual summary of performance against the standards.

5. Equality and Diversity

- 5.1 We are committed to fairness and equality for all regardless of their colour, race, ethnicity, nationality, gender, sexual orientation, marital status, disability, age, religion or belief, family circumstances or offending history as defined in our relevant Group policies. Our aim is to ensure that our policies and procedures do not create an unfair disadvantage for anyone, either directly or indirectly.

6. Monitoring and Review

6.1 The next policy review is scheduled for April 2021 and then every two years thereafter.

The following performance standards, performance indicators and records will be maintained in pursuance of this Policy. Compliance with the GDPR and this Policy will be monitored by the GDPR Forum receiving quarterly updates. An annual summary of Performance Indicators will be presented to Platform Housing Group's board.

Area	Standard/Record	PI
Subject Access Requests	Provide all disclosable personal information within one month	Number of SARs. Average number of calendar days.
Programme of Data Compliance Checks based on risk	Clear outcome report with improvement plan and lessons learned logged for each audit	No. of completed compliance checks in year
Data Breach identification and management	Clear outcome report with improvement plan and lessons learned logged for each reported breach	No. of reported breaches for year
Information Asset Register	Record of all Information Systems and Sharing Agreements held within Platform Housing Group to be comprehensively recorded in a central database including Information Owner, purpose, security measures and review date.	N/A
ICO Registrations	Annual Registration for Platform Housing Group, Fortis Property Care and any other trading companies in the Group. Record of Registrations, review date, fee paid on annual basis.	N/A
Data Protection Training	All roles : Completion of Induction Training All Roles *:	Exception based number of staff who have not completed any GDPR training in last 2 years.

	E-learning covering GDPR & Computer Security (* Except where limited access to personal data where self- study basic training materials will be used)	
--	--	--

7. Associated Documents / Policies

7.1 List of documents/associated policies/publications.

- Data Protection Act 1998
- Human Rights Act 1998
- Information Commissioner’s Office (ICO) Code of Practice
- HCA Regulatory Framework for Social Housing in England
- NHF guidance on data retention periods
- General Data Protection Regulation
- Platform Group Disciplinary Policy
- Group Data Protection Procedure
- Group Information Security Policy
- Group Data Rights Policy
- Group Consent and Data Rights Procedure
- Group Data Breach Policy

Author:	Colin Bailey
Version:	Live
Release date:	January 2019
Next Review date:	April 2021
Document type:	Policy
Approved by:	GET
EIA Completed (where required):	
Customer consultation: (where appropriate)	N
Employee Handbook amends: (where appropriate)	N