Paragon Asra Housing Limited

Data Protection Policy

November 2022

Owning manager	Manjeet Johal - DPO
Department	Governance
Approved by Board	November 2022
Next review date	November 2025

	Contents	Page

Paragon Asra Housing Limited (PA Housing) is committed to equality and diversity. This policy has considered the Equality Act 2010 and its protected characteristics which are: race, gender, gender reassignment, disability, religion or belief, sexual orientation, age, marriage, civil marriage and partnership, pregnancy, and maternity explicitly. We will make sure that all of our communication is fully accessible and to achieve this if a policy or document needs to be available in other formats, we will provide them.

AUDIT LOG

Date of Change	Who updated	Details of the change
18/10/17 – V11	BA	To reflect changes made in UK DP Bill published Sep 2017
29/11/17 – V12	BA	Amendments following three papers released by the Article 29 working party (WP250-252).
27/12/17 – V13	BA	To include changes suggested by Mandy Webster of Data Protection Consulting Limited
6/3/18 – V14	BA	To include changes from Devonshires review
13/3/18 – V15	BA	Revised lawful basis section 5 reflecting MW, FR and BA discussion.
March 2020	Linda Gove	Revised to take account of recent advice. Devonshires advice incorporated into this version
November 2021	Manjeet Johal	Document was due for review. Document revised, updated with new DPO details and new review date set.
October 2022	Manjeet Johal	Document due for review. Revised and reviewed by Devonshires with their changes incorporated into this version mainly around section 14.

1. Introduction

1.1 Everyone has rights about the way in which their personal data is handled. During our activities we will collect, store and process personal data about our residents, employees, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful service delivery.

1.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

1.3 Data protection law is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

2. Policy Statement

2.1 The types of personal data that Paragon Asra Housing Limited ('PA Housing') may be required to handle include information about current, past, and prospective residents, employees, Board members, suppliers, third parties and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the UK General Data Protection Regulation (the Regulation), the Data Protection Act 2018 (the Act) and other regulations related to personal data (together referred to as the 'Data Protection Legislation' in this policy).
The Data Protection Act 2018 was amended on 1 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

2.2 PA Housing is registered with the Information Commissioners Office as a Data Controller (registration number ZA225289) and ensures that its handling of personal information is of a high standard.

2.3 Data Protection Legislation is enforced by the Information Commissioners Office which has extensive powers to take action against organisation which breach data protection law. This includes substantial fines as well as other regulatory action such as enforcement notices.

Personal data we hold will not be sold to any other organisation or individual.

2.4 Data privacy issues will be considered as part of the Risk Management Strategy, and if assessed as a priority risk area the commitment of resources will be considered to attend to the controls to mitigate these risks.

3. Scope

3.1 All processing of personal data is governed by the Data Protection Legislation. The Data Protection Legislation applies to all personal data - whether held on a computer or similar automatic system or whether held as part of a structured manual filing system.

3.2 For us to deliver our services, we collect and process personal data for specific purposes which we will inform our data subjects about. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive

from other sources (including, for example, partner organisations, local authorities, central government, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

3.3 Processing relates to collecting, editing, and updating, retaining, and storing, disclosing or sharing, deleting / erasing and destroying, viewing (including images and video footage), archiving, and listening to personal data

3.4 Personal data relates to any information relating to an identified or identifiable natural person. This includes any expression of opinion about the individual.

3.5 The processing of sensitive personal data shall be proportionate to the aim being pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

4. Responsibility

4.1 Whilst everyone who processes personal data is responsible for complying with the policies, procedures and regulations, overall responsibility for personal data rests with the Board.

4.2 The Board is responsible for ensuring data protection by default and by design and supports the data protection rights of all PA Housing stakeholders and compliance with all relevant legislation and regulatory requirements.

4.3 The Executive Management Team is responsible for the management of personal data, ensuring good practice and that compliance with legislation, policies, procedures, and regulations can be demonstrated. This includes:

- development and implementation of this policy
- security and risk management in relation to compliance with this policy

4.4 Executive directors, managers and supervisors are responsible for developing and encouraging good information handling practices.

4.5 Compliance with legislation, policies, procedures, and regulations is the responsibility of all employees who control or process personal data.

4.6 Employees are responsible for ensuring that their own personal data is accurate and up to date.

4.7 The DPO will be responsible for:

- Understanding and communicating legal obligations
- Identifying potential problem areas or risks
- Keeping the Board updated about data privacy responsibilities, risks and issues
- Producing and reviewing all data privacy procedures and policies on a regular basis
- Providing appropriate training and advice for all staff members
- Answering questions on data privacy from staff, board members and other stakeholders
- Liaising with the Information Commissioner’s Office on relevant cases and issues

5. Data Protection Principles

5.1 Anyone processing personal data must comply with the seven principles of good practice. These provide that personal data must be:

- Processed fairly, lawfully, and transparently
- Collected for explicit, legitimate purposes and not processed further than stated to the subject
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and up to date
- Not kept in an identifiable form for longer than necessary for the purpose
- Secure and monitored
- The controller must be able to demonstrate compliance with the UK GDPR's other principle of accountability

5.2 For personal data to be processed lawfully, they must be processed based on one of the legal grounds set out in the Regulation. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, necessary to protect the vital interests of the data subject or necessary to carry out tasks that are in the public interest.

5.3 When special category data is being processed, additional conditions must be met as set out in Article 9 of the Regulation and Schedule 1 and 2 of the Data Protection Act 2018. When processing personal data as data controllers during our business, we will ensure that those requirements are met. A contract must be in place with all data processors and that this will be compliant with Data Protection Legislation.

5.4 A record of all processing activity will be maintained by those responsible for holding data. This will include personal data that we are chiefly responsible for as well as all data processed for a third party, and document all transfers, security processes, legal bases for processing and locations of storage.

5.5 We will maintain a standard of privacy by design, by which all new projects, services and changes will be built with privacy and data protection as a key consideration. This includes undertaking a data privacy impact assessment (DPIA) for all processing that is considered to be high risk.

5.6 We shall provide a privacy notice to all data subjects at the point at which we collect their data, informing them of our intentions to process their data and how we intend to do it. This must be specific for the processing operation.

5.7 We will only process personal data for specific purposes or for any other purposes specifically permitted by the Regulation or the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

6. Data Subjects' Rights

6.1 Under the UK GDPR individuals have the following rights regarding data processing:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.

- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- To not have significant decisions made solely by automated process that will affect them.
- To sue for compensation if they suffer damage by any contravention of the UK GDPR or any other data protection laws.
- To take action to rectify, restrict, erase, including the right to be forgotten, or destroy inaccurate data.
- To have the right to complain.
- To request the supervisory authority to assess whether any provision of the UK GDPR has been contravened.
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- To object to any automated profiling that is occurring without consent.

7. Consent

7.1 Consent is defined in the European Directive 95/46/EC as "any freely given, specific, informed, and unambiguous indication of an individual's wish by which the data subject signifies his agreement to personal data relating to him being processed". The data subject can withdraw their consent at any time.

7.2 PA Housing understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be valid basis for processing.

7.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. PA Housing must be able to demonstrate that consent was obtained for the processing operation.

7.4 For sensitive data and for the purpose of direct marketing, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

7.5 In most instances, consent to process personal and sensitive data is obtained routinely through emails e.g., when a requestor replies or indicates in an email that they are happy to receive marketing related materials.

8. Notifying Data Subjects

8.1 If we collect personal data directly from data subjects, we will inform them about:

- The purpose or purposes for which we intend to process that personal data
- The third parties or types of third parties, if any, with which we will share or to which we will disclose that personal data
- The means, if any, with which data subjects can limit our use and disclosure of their personal data
- The legal basis we have for processing data
- The identity and contact details of the data controller, the data protection officer, and any other parties relevant to the processing of their data
- The length of time we intend to retain the data for (or, if not known, the

methodology used to determine the retention period)
- The use of automated decision making or profiling (automated processing of personal data to evaluate certain things about an individual) where applicable

8.2 We will also inform data subjects whose personal data we process that we are the data controller with regards to that data, and the contact details of the Data Protection Officer.

9. Adequate, relevant, and non-excessive processing

9.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject and within their reasonable expectations.

10. Accurate Data

10.1 We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data 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 data.

11. Timely Processing and Retention

11.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

11.2 Anonymous personal data may be kept for statistical use, for example, equality and diversity opportunities.

12. Processing in-line With Data Subject's Rights

12.1 We will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any data held about them us
- Ask to have inaccurate data amended
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.
- Move, copy, or transfer easily from one database to another safely and securely without hindrance to usability
- Be informed on the nature of the processing taking place, using tailored privacy notices specific to each service provided to them

13. Data Security

13.1 We will process all personal data we hold in accordance with our ICT Policy.

13.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if it agrees to comply with those procedures and policies, or if it puts in place adequate measures itself. Sub-processors will not be appointed without our approval.

13.3 We will maintain data security by protecting the confidentiality, integrity, and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed
- Availability means that authorised users should be able to access the data if they need it for authorised purposes.

14. Transferring Personal Data to a Country Outside The EEA

14.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the UK GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".
The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply.

14.2 We may only transfer Personal Data outside the UK if one of the following conditions applies:
(a) the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;
(b) appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
(c) the Data Subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or
(d)the transfer is necessary for one of the other reasons set out in the UK GDPR including:
(i) the performance of a contract between us and the Data Subject;
(ii) reasons of public interest;
(iii) to establish, exercise or defend legal claims;
(iv) to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent; and
(v) in some limited cases, for our legitimate interest.

14.3 Whilst most of the IT systems that we use are based within the UK or Europe, we do use the following, which means that data may be stored electronically outside of the UK and Europe.
- Survey Monkey
- Microsoft Cloud
- Google
- Apple

15. Disclosure and Sharing of Personal Information

15.1 We will share personal data we hold across our services in accordance with the privacy statement provided to data subjects, either at the point of initial contact or via our website.

15.2 We will also disclose personal data we hold to third parties:

This may include contractors (processors) who work for us to deliver our services; a contract will be in place with all data processors and that this will be compliant with the Data Protection Legislation Disclosures to another third-party organisation may

be made under an external data sharing agreement.

15.3 In some cases, we may be under a duty to disclose or share a data subject's personal data in order to comply with a legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, or others. This includes exchanging information with other organisations for the purposes of fraud prevention and credit risk reduction.

16. Subject Access Requests and Breaches

16.1 Subject Access Requests will be dealt with and processed in accordance with our Subject Access Request Procedure.

16.2 Any reasonable request for personal data from a data subject will be processed in accordance with the Regulations.

16.3 When receiving enquiries, if we have any doubts as to the identity of the applicant, we will request the applicant's identity to make sure that information is only given to the person entitled to it.

16.4 Data Breaches will be processed in line with our data breach notification procedures. The ICO will be notified of any significant data breaches which meets the statutory test in the Regulation within 72 hours.

16.5 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service.

17. Training and Review

17.1 This policy will be made available for viewing on PA Housing's website and all current tenants and those applying for accommodation, together with current and prospective employees and current and prospective Board members will be guided towards this policy so that they may see how personal data collected may be used by us and who this data may be shared with.

17.2 All staff will receive training and refresher training on this policy and on the associated procedures, in particular when there has been a substantial change in the law or in our policy and procedures.

17.3 New staff joiners will receive training as part of their induction process.

17.4 Internal audit procedures will form an important part of establishing and sustaining good data privacy practices.

18. Changes to this Policy

18.1 We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail, email or via our website.

18.2 This Policy aims to protect and promote the rights of data subjects and should be read in conjunction with the following:

Document and Data Retention Policy
Customer Privacy Notice Colleague
Privacy Notice
Subject Access Request Procedure
Personal Data Breach Procedure
Data Sharing Procedure
DPIA Procedure
ICT Security Policy

Appendix 1 – Definitions

A1.1 **Breach of personal data** – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the ICO, dependent on the seriousness, and where the breach is likely to adversely affect the personal data or privacy of the data subject.

A1.2 **Child -** the UK DP legislation defines a child as anyone under the age of 13 years old. We may rely on any of the bases given in Article 6 of Article as our lawful basis for processing a child's personal data. However, for some of the bases there are some important additional considerations that we need to take into account when the Data Subject is a child.

A1.3 **Consent by Data subject -** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

A1.4 **Data Controller** – the natural or legal person, public authority, agency or other body which determines the purposes and means of the processing of personal data.

A1.5 **Data subject** – any living individual who is the subject of personal data held by an organisation.

A1.6 **Filing system** – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. 'Structured' covers any form of computer system or manual system which has a 'fast indexing' system.

A1.7 **Material scope –** DP legislation applies to the processing of personal data wholly or partly by automated means, (i.e. by computer) and to the processing other than by automated means of personal data, (i.e. paper records) that form part of a 'structured' filing system or are intended to form part of a filing system.

A1.8 **Personal data** – any information relating to an identified or identifiable natural person, ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. It covers information about living people stored on a computer or in an organised paper filing system, CCTV system, digital camera or audio recordings and digital images.

A1.9 **Processing -** is any form of automated processing of personal data intended to

evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

A1.10 **Profiling** – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

A1.11 **Special categories of personal data** – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. (Special categories is similar to the previous (UK DP Act 1998) Sensitive categories with some additions.)

A1.12 **Supervisory Authority** – the independent public authority in the UK established to administer and regulate DP law. This is the Information Commissioner's Office – ICO.

A1.13 **Third party** – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.