Paragon Asra Housing Limited

Data Protection Policy

May 2018

Owning manager	Barry Alford
Department	ICT
Approved by Board	22 March 2018
Next review date	March 2021

	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.

1. Introduction

The General Data Protection Regulation (GDPR) of 2016 will be effective from 25 May 2018 and completely replaces all previous Data Protection (DP) laws. Its purpose is to protect the 'rights and freedoms' of living individuals and to ensure that personal data is not processed without their knowledge and is processed with their consent.

The GDPR has been accepted as DP Protection law in the United Kingdom with some extensions - as laid down in UK Data Protection Act 2018. The term 'DP legislation' is used in this policy to denote the collective Data Protection law (of GDPR and UK Act) effective from 25 May 2018. All DP legislation in the UK is regulated by a supervisory authority called the Information Commissioner's Office (ICO).

The DP legislation introduces a number of new concepts and improvements to data subjects' rights. A summary of the regulation is given below:

- gaining explicit consent from data subjects for the use of their personal data;
- processing relevant and adequate personal data, only where this is strictly necessary for legitimate organisational purposes;
- collecting only the minimum personal data required for these purposes and not processing excessive personal information;
- providing clear information to individuals about how their personal data will be used and by whom;
- processing personal information fairly and lawfully;
- maintaining an inventory of the personal data categories that are processed;
- personal data is accurate and, where necessary, up to date;
- retaining personal data only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes;
- keeping all personal data secure;
- only transferring personal data outside the EU in circumstances where it can be adequately protected or where equivalent standards apply;
- the application of the various allowable exemptions;
- the requirement to appoint a Data Protection Officer (DPO) in some circumstances;
- 'special categories' of personal data (previously sensitive personal data) is extended to include biometric and genetic data;
- mandatory reporting of data breaches or data loss in some circumstances;
- enhanced security of personal data, e.g. encryption and anonymisation;
- respecting a subject's access rights, including new provisions such as data portability.

Appendix 1 lists a number of definitions.

2. Policy statement, objectives and scope

Paragon Asra Housing Ltd (PA Housing) is a controller under DP legislation - for personal data processing and makes decisions about how and why it is processed. It is committed to compliance with all DP legislation and the protection of the 'rights and freedoms' of individuals whose information PA Housing collects and processes.

The policy's objectives are to:

- protect the personal data interests of individuals and other key stakeholders by the use of appropriate procedures and controls;
- provide the supporting framework for achieving and maintaining compliance;
- ensure PA Housing meets applicable statutory, regulatory, contractual and/or professional duties.

PA Housing necessarily and routinely uses personal data information when it carries out many aspects of its day to day business. The organisation is subject to this policy, with some requirements spreading out and imposing responsibilities on partner organisations, e.g. our maintenance contractors. (Typically they are a Data Processor of personal data that we have collected in our role of Data Controller).

Personal data is all data within our computer systems, including our Housing Management System, Document Management System, email, Word documents, Excel worksheets, plus manual structured filing systems that refer to a living Data Subject. (A structured filing system is defined as having a form of index enabling fast and easy access to individual documents within it. A filing system in just date order, without any such index, would not be considered a structured system). If there is any doubt as to whether a paper filing system is within scope of DP law, the DPO will provide guidance.

Special categories of personal data are considered to be more sensitive and so need more protection. These include racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

This policy applies to all of PA Housing's personal data processing functions, including those performed on personal data and any other personal data processed from any source, relating to:

- customers (applicants and residents, whether renting or purchasing property);
- clients (any organisation or person(s) to whom we provide a service);
- suppliers and partners (contractors, local authorities and stakeholders);
- our employees.

Any breach of DP legislation or this policy by employees will be dealt with under the Disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

The Board of PA Housing is ultimately responsible for compliance with relevant laws and is responsible for risk management.

PA Housing is required to designate a DPO, who is responsible for reviewing annually the register of processing in light of any changes to PA Housing's activities, management review or any additional requirements identified by means of Data Protection Impact Assessments.

Partners and any third parties working with PA Housing who may have access to personal data, will be expected to have read, understood and comply with the requirements and agreements in our Data Protection – Supplier Tender Clause and Agreement policy. This policy imposes obligations on the third party that are no less onerous than those to which PA Housing is committed, and gives us the right to audit compliance with the Supplier's agreement.

All employees are responsible for compliance with PA Housing policies and procedures.

3. Data Protection principles

We are committed to ensuring that we comply with the six data protection principles and the other requirements of GDPR, as follows:

1. Personal data must be processed lawfully, fairly and transparently.
2. Personal data can only be collected for specified, explicit and legitimate purposes.
3. Personal data must be adequate, relevant and limited to the purpose for which the data is processed.
4. Personal data must be accurate and kept up to date.
5. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for the processing purposes.
6. Personal data must be processed in a manner that ensures the appropriate security.

4. Data subjects' rights

4.1 Data Processing

Data subjects have the following rights regarding data processing and the data that is recorded about them:

- to make subject access requests regarding the nature of information held and to whom it has been disclosed. A number of exemptions apply whereby personal data does not have to be disclosed – see the Subject Access Request procedure;
- to prevent processing for purposes of direct marketing;
- to be informed about the mechanics of automated decision-taking processes that will significantly affect them;
- not to have significant decisions that will affect them taken solely by automated processes;
- to sue for compensation if they suffer damage by any contravention of DP law;
- to request the ICO to assess whether DP law has been contravened;
- to have personal data provided to them in a structured, commonly used and machine-readable format, and the right, in certain circumstances, to have that data transmitted to another controller;
- to object to any automated profiling that is occurring without consent;
- to take action to rectify, block, erase or destroy inaccurate data;

- in certain circumstances, to be forgotten.

The last two sets of rights are dealt with in more detail in Appendix 3 – Data Subjects' rights – details.

4.2 Complaints

Data subjects who wish to complain about how their personal data has been processed may:

- use the Complaints policy;
- complain directly to the DPO;
- complain to the ICO.

5. Lawful basis for processing

5.1 Personal data

PA Housing will only collect and process personal data if one of the conditions set out below has been satisfied:

- the express consent of the tenant or employee is obtained prior to the processing of personal data. Consent must be freely given; it must also be specific and informed. It must be given by an unambiguous statement or by clear affirmative action signifying the data subject's agreement to the processing. In practice this means that wherever possible consent should be obtained in writing and signed by the subject with clear wording in plain English explaining precisely what they are agreeing to. Where written consent is not possible, verbal consent can be given but the terms of the consent must be clearly given to the subject and a written record of the consent kept;
- processing is necessary for the performance of a contract to which the tenant or employee is party or in order to take steps at the request of the tenant or employee prior to entering the contract;
- processing is necessary for compliance with a legal obligation to which PA Housing is subject;
- processing is necessary in order to protect the vital interests of the tenant or employee or of another natural person;
- processing is necessary for the purposes of the legitimate interests pursued by PA Housing or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the tenant or employee which require protection of personal data, in particular where the data subject is a child.

5.2 Special categories of personal data

PA Housing will only collect and process special categories of personal data if one of the conditions set out below has also been satisfied:

- the data subject has freely given explicit consent to the processing of their personal data for one or more specified purposes;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment law and the controller has an appropriate policy document in place;

- processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent;
- processing relates to personal data which has been made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest. The only categories in this subsection potentially relevant to PA Housing are the administration of justice, (i.e. providing information to the Court or those pursuing proceedings and preventing or detecting unlawful acts);
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, including the need to complete statutory or regulatory returns.

5.3 Lawful bases for PA Housing

Up to 24 May 2018 our lawful basis for processing is that we obtain the consent of residents to use their personal data. However the way that consent has been handled historically will not satisfy the more stringent requirements of the new DP legislation and we must use different bases for processing.

We'll use two different lawful bases dependent on the circumstances:

- We process residents' personal data 'for the purposes of legitimate interests' of providing and maintaining our properties.
- Where we have a contract with our tenants, we process personal data in order to fulfil it.

The different requirements for the processing of special categories of personal data means that 'legitimate interests' cannot be used as the sole lawful basis and there must an additional lawful basis.

We therefore use two additional lawful bases for special categories dependent on the processing requirement:

- In order to provide some of our services we need explicit consent by the resident. (It should be recognised that if consent was withdrawn the customer would exclude themselves from those services).
- For completion of statutory and regulatory returns, our lawful basis is "statistical purposes in accordance…….with Member State law".

Personal information about employees and tenants, especially information in special categories, is shared only with staff who need to know the information in order to carry out their legitimate duties. This may involve sharing information between individuals in different departments and where appropriate PA Housing sets up

protocols to clarify how this operates.

Where online services to children (defined as under the age of 13) are provided, parental or custodial authorisation must be obtained.

6. Responsibilities under the Data Protection law

6.1 General responsibilities

PA Housing is a data controller and in some circumstances a data processor, e.g. we provide housing management services to a small amount of housing stock owned by other Registered Providers.

The Board is ultimately responsible for ensuring that PA Housing does not collect information that is not strictly necessary for the purpose for which it is obtained.

Executive directors, managers and supervisors are responsible for developing and encouraging good information handling practices. Responsibilities are set out in role profiles.

Compliance with DP legislation is the responsibility of all employees who control or process personal data.

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

Customers who will be providing personal data will need to be shown the Fair Processing Notice at an appropriate point.

6.2 Executive Management Team

With the guidance and advice of the DPO, the Executive Management Team is responsible for the management of personal data, ensuring good practice and that compliance with DP legislation can be demonstrated. This includes:

- development and implementation of this policy;
- security and risk management in relation to compliance with this policy;
- having data protection expertise;
- undertaking an annual review of personal data held to ensure that there is a sound business reason for holding that information.

Directors and senior managers have equivalent responsibility and accountability for the control of personal data within their area of responsibility.

The DPO has specific responsibilities for designing procedures such as for Subject Access Requests. These will be handled by other staff but the DPO will provide staff with clarification on any aspect of DP legislation and compliance.

6.3 Accountability

The new DP legislation introduces the principle of accountability which states that the Data Controller is not only responsible for ensuring compliance but also for demonstrating that each processing operation complies with DP legislation. Specifically, Data Controllers are required to evidence compliance with the Regulation, which includes:

- maintaining necessary documentation of all processing operations;
- implementing appropriate security measures;
- carrying out Data Processing Impact Assessments (DPIAs);
- complying with requirements for prior notifications, or approval from supervisory authorities;
- appointing a DPO, if required.

7. Notification

PA Housing has notified the ICO that it is a Data Controller and processes certain information about data subjects. PA Housing has identified all the personal data that it processes and this is contained in the Data Processing and Purposes log.

A copy of the ICO notification (the register entry) is retained and renewed annually by the DPO. Any changes to PA Housing's activities, (e.g. from DPIAs) are notified by the DPO.

8. Disclosure of data

8.1 Exemptions

DP legislation permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (including health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, e.g. emergency medical situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork to justify the decision and all such disclosures must be specifically authorised by the DPO.

This exemption allows the release for the stated purposes and does not cover the disclosure of all personal data in all circumstances. The following types of verification and limitation questions must be asked:

- Is the person requesting the information who they say they are?
- Is their intention to prevent or detect a crime, catch or prosecute an offender or assess or collect tax or duty?
- If the information is not released, will this significantly harm prevention of a crime or catching of a suspect? (The risk must be that the investigation may be impeded.)
- What is the minimum amount of information to enable them to do their job?
- What else needs to be known to be sure that the exemption applies?

8.2 Information sharing

PA Housing must ensure that personal data is not disclosed to unauthorised third parties. This includes family members, friends, government bodies and in certain circumstances the police. All employees should exercise caution when asked to disclose personal data held on an individual to a third-party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of PA Housing's business.

We have certain Information Sharing Agreements in place, e.g. with the police, councils and other agencies using set sharing protocols.

Board members do not have any right to see personal data stored on files, except with the written permission of the individual, or any information that would not be disclosed to the individual, except as is necessary in the course of their duties.

There are situations where information will be withheld, such as where it would identify someone else who has not given consent to the disclosure, unless it can be edited out (redaction). Joint tenants will be asked if they agree to their data being disclosed to the 'other' tenant if only one makes the request. Otherwise all of the references to the other joint tenant will have to be redacted. There may be other exemptions specifically relating to health information.

If there are concerns that the DP legislation would be broken, a court order requiring the release will be requested and the DPO will advise on this.

8.3 Safeguarding information

PA Housing actively works to safeguard children, young people and vulnerable adults from harm. PA Housing has a duty to tell Social Services where an individual's safety is at risk and share information with them, whether reported directly or indirectly to staff. The types of information that may be shared include names, contact details, information about a person's physical or mental health and relations with others.

PA Housing has detailed procedures that cover the reporting of this information which follow various local safeguarding information sharing protocols. PA Housing expects its staff to immediately report any concerns to the safeguarding lead who will report the information in accordance with the Safeguarding policy.

In certain limited circumstances DP legislation provides for personal data, even sensitive data, to be shared without the individual knowing about it.

9. Direct marketing

PA Housing may use personal data for direct marketing (including to business partnerships) in relation to its activities. This includes email and text, phone calls and direct mailshots. Consent will be obtained at the time that personal data is provided by the individual. Any individual can exercise their right, at any time, to opt out of their personal data being used in this way and PA Housing will accord with their request.

Our computer systems record the contact preferences of residents (if and how) which, of course, will be followed.

The EU e-privacy directive is due to be replaced shortly by the e-privacy regulation to apply from May 2018, although this has not yet been approved by the European Commission. Financial penalties will be increased to match the GDPR level of fines. We may require consents to be renewed.

10. Employees

Personal data relating to employees is obtained from job applications and whenever data is refreshed through the HR department or Payroll. The job application form states that the information collected will be strictly confidential and used only for the purposes of personnel and salary administration, or otherwise in connection with PA Housing's business. This includes using data for monitoring purposes, and checking email and internet use and checking CCTV for health and safety purposes in the case of an incident. This also appears in contracts of employment. Data will not be kept any longer than is necessary.

PA Housing will comply with the following requests for personal data:

- from agents authorised by the employee, e.g. mortgage requests, references. The employee should confirm in writing that the information is to be released;
- for law enforcement (i.e. by the police for the prevention or detection of crime, assessment or collection of any tax or duty by HM Revenue and Customs or the Child Support or Child Maintenance Agency). Disclosure is only allowed where failure to make the disclosure is likely to prejudice one of these purposes. In all cases the purpose of the request will be obtained in writing;
- if urgently required, for the prevention of injury and damage to health;
- by trade union officials. The employee will be asked to confirm in writing;
- for any other compulsory legal process;
- by specifically identified external sources, e.g. pension administrators, in order to administer internal benefit schemes.

Employees are entitled to see their personal data, but need to give HR reasonable notice to provide access. Employees are also entitled to know the purposes for which their personal data is intended to be used and the likely recipients (or class of recipients). The following information is excluded from disclosure:

- parts of references received that identify third-parties and the third-party does not consent to the disclosure and we decide on a balance of interests that it is right to withhold the information;
- personal data used for management forecasting or planning if disclosure is likely to prejudice the conduct of that business or activity only;
- records relating to any negotiations with the employee if disclosure is likely to prejudice those particular negotiations;
- if it involved disclosing information relating to an identifiable third party, unless the third party has consented or it is reasonable to comply without their consent. Failing these options, the data will be edited ('redacted') to protect the identity of third parties. Disclosure will be made if a health record is sought and the third party is a health professional who has compiled or contributed to it.

An employee will not be able to prevent processing necessary for the performance of a contract to which the employee is a party.

Personal data about an employee given to board members will be edited to remove any third-party information.

11. Suppliers and contractors

PA Housing employs various contractors to carry out tasks and services on its behalf; some have a genuine need to use personal data of our residents. Such contractors are known as data processors.

If a contractor is likely to be a data processor, a standard set of clauses must be included in the tender document. These state basic requirements needed on the data protection status of the contractor. Full details are given in the Data Protection – Supplier Tender Clause and Agreement policy.

The contractor who is successful in winning the contract must enter into a Data Protection Processing Agreement that sets out the standards and obligations that PA Housing expects in the processing of personal data. This longer agreement is also in the Data Protection – Supplier Tender Clause and Agreement policy.

12. Risk and Data Protection Impact Assessment

There may be risks associated with the processing of particular types of personal data and particular circumstances, which PA Housing must assess by means of a DPIA. A DPIA can cover in-house processing of personal data and that undertaken by other organisations on behalf of PA Housing. See the Data Protection Impact Assessment procedure.

New systems and technologies should be subject to examination that they have been designed to meet DP requirements; if not additional controls may be necessary. If the scope, nature, context and purposes of the processing are likely to result in a high risk to rights and freedoms, PA Housing shall, prior to the processing, carry out a DPIA of the effect of the envisaged processing. A single DPIA may address a set of similar processing operations that present similar high risks. The DPO must be

involved in all DPIAs.

Where, as a result of a DPIA it is clear that PA Housing is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not PA Housing may proceed must be reviewed by the DPO. The DPO shall, if there are significant concerns, escalate the matter to the ICO.

Appropriate controls may be selected from ISO27001 (a set of Information security standards) and other good practice sources to reduce the risk to an acceptable level and reach DP compliance.

In order to protect employees and contractors from risk when working in residents' homes, PA Housing has a system to identify people who may threaten the safety of employees and others. This information is confidential and will not be disclosed outside PA Housing unless it is required to ensure the health and safety of contractors and other suppliers. It will be subject to review and kept up to date and accurate.

13. Security breaches

A 'personal data breach' firstly involves a security incident, which leads to compromise of data integrity, availability or confidentiality.

Examples of security incidents include:

- Poor security
  - cyber security breach by access via a user account;
  - access to a global email server via an administrator's account;
  - ransomware;
  - misuse of passwords.

- Data accidentally published
  - employee sends email with personal data asking for technical assistance;
  - email sent to wrong recipient;
  - paper files circulated with too much information included;
  - intranet information accidentally goes on website.

- Hacked
  - hacking;
  - hacking using forged cookies.

- Inside job
  - social engineer poses as CEO and emails HR for information on employees;
  - employee under notice resets all network servers to factory default settings and disconnects remote backups;
  - employee copies protected data onto an external disk;
  - malicious employee - passes employee login to hackers;
  - malicious employee - publishing HR data to internet.

- Lost/stolen device or media
  - stolen laptop unencrypted;
  - decommissioned hard drives not ‘scrubbed’ but sold on second hand;
  - CDs lost in post unencrypted.

Any employee who suspects a data protection breach must report it immediately to their management who will liaise with the DPO. An investigation will likely take place, following discussion with the Executive Director of Governance and Company Secretary. Serious breaches will be reported to the ICO using the Breach Notification procedure.

14. Records and housekeeping

14.1 Data Processing Purposes Log

PA Housing has established this log to record processing activities of personal data, defining:

- purpose of the processing;
- the various steps involved in the processing;
- what data is being processed;
- who the data relates to;
- technical and organisational measures taken to secure the data;
- how consent is given and the lawful processing basis used.

Full details are given in the separate Data Processing Purposes Log procedure.

14.2 Retention and disposal of data

PA Housing shall not keep personal data in a form that permits identification of data subjects for longer than it deems necessary (in relation to the purpose(s) for which the data was originally collected).

PA Housing may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out in the Document and Data Retention policy, along with the criteria used to determine this period including any statutory obligations to retain the data.

Personal data must be disposed of in a way that protects the “rights and freedoms” of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with the Document and Data Retention policy.

15. Training

All staff and board members will be required to read and understand this policy as

part of their induction. Staff will be trained on a regular basis on this policy, including about their own rights. More detailed training on handling subject access requests in accordance with DP legislation will be given to relevant staff. The DPO will receive more specialised training.

16. Monitoring and reporting

The DPO monitors compliance with this policy and reports any breaches to the Executive Director of Governance and Company Secretary. PA Housing considers all personal data provided by its customers, staff or contractors as confidential, and any unauthorised disclosure is treated very seriously.

Deliberate breach of the policy is considered a serious disciplinary offence and may result in disciplinary action being taken which may in turn lead to dismissal. Staff may also face criminal liability in certain circumstances. Employees are required to notify the DPO where a breach of policy is suspected.

17. Linked policies

Complaints
Customer Privacy (and Fair Processing Notice)
Data Protection – Supplier Tender Clause and Agreement
Disciplinary
Document and Data Retention

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. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the 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 **Establishment –** the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

A1.7 **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.

A1.8 **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.

A1.9 **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.

A1.10 **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.

A1.11 **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.

A1.12 **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.)

A1.13 **Supervisory Authority** – the independent public authority in the UK established to administer and regulate DP law. This is the Information Commissioner's Office – ICO.

A1.14 **Territorial scope -** the GDPR will apply to all controllers are established in the European Union (EU) who process the personal data of data subjects. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU. The GDPR has effectively been enshrined in UK law in the 2017 Data Protection Bill, albeit with a few additions and changes.

A1.15 **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.

Appendix 2 – Data Protection Principles

A2.1 Personal data must be processed lawfully, fairly and transparently.

Lawfully
A lawful basis must be identified before personal data is processed.

Fairly

In order for processing to be fair, the Data Controller has to make certain information available to the data subjects. This applies whether the personal data was obtained directly from the data subjects or from other sources, (e.g. a local authority).

Transparently

Transparency means we need to keep people informed about what we plan to do with their personal data. We do this by way of a Fair Processing Notice which must be detailed, specific, understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language. (See PA Housing's Customer Privacy policy and Fair Processing Notice.)

Specific information provided to the data subject must, as a minimum, include:

- the identity and contact details of the controller and the controller's representative, if any;
- the contact details of the DPO;
- the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- that the controller intends to transfer personal data outside the European Economic Area, where applicable, and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

A2.2 Personal data can only be collected for specified, explicit and legitimate purposes.

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner's Office as part of PA Housing's DP registration. PA Housing's registration reference is ZA225289 and details of the registration entry may be seen on the ICO's website. (This may not be the case when the register becomes 'private' from April 2018).

Where there is a change in purpose, other than the original purpose, and prior to

further processing we must:

- provide the data subject with information on the new purpose
- obtain consent for that new purpose.

All employees must keep the DPO informed of new developments that might cause a change of purpose and hence a requirement for new consent.

A2.3 Personal data must be adequate, relevant and limited to the purpose for which the data is processed.

All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and will be checked by the DPO.

If data is given or obtained that is excessive or not specifically required by PA Housing's documented procedures, the relevant line manager is responsible for ensuring that it is securely deleted or destroyed in line with the Document and Data Retention policy. The DPO will confirm the secure deletion in a follow-up check.

A2.4 Personal data must be accurate and kept up to date.

Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

Whilst our customers and staff should notify us of any changes in circumstance, regular proactive collection and checking campaigns will be necessary. It is the responsibility of PA Housing to ensure that any notification regarding change of circumstances is noted and acted upon.

The DPO is responsible for ensuring that:

- At least annually the retention dates of all the personal data processed by PA Housing are reviewed by line management to identify any data no longer required and arranging secure deletion/destruction.
- We respond to requests for rectification from data subjects within one calendar month. If PA Housing decides not to comply with the request, the DPO must respond to the data subject to explain the reasoning and inform them of their right to complain.
- We make appropriate arrangements where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is not to be used to inform decisions about the individuals concerned and for passing on any corrections.

A2.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for the processing purposes

Personal data will be retained in line with our Document and Data Retention policy. Once its retention date is passed, it must be securely destroyed.

Where personal data is retained beyond its retention date, it should be 'obfuscated' by being minimised, encrypted or pseudonymised in order to protect the identity of the

data subject. This is dependent on the technical capabilities available.

The relevant line manager must specifically approve in writing any data retention:

- that exceeds the retention periods and
- ensure that the justification is clearly identified in line with GDPR.

The DPO will check the approval, the reasons for it and that it is appropriate.

A2.6 Personal data must be processed in a manner that ensures the appropriate security.

The relevant line manager is responsible for ensuring that risks are assessed and measures are in place to ensure appropriate security. In some cases this will need specialist assistance, e.g. from the ICT team or an audit function.

The DPO will check risk assessments and the appropriateness of control measures.

In determining appropriateness, the line manager will also consider the extent of possible damage or loss that might be caused to individuals if a security breach occurs; the effect of any security breach on PA Housing; and any likely reputational damage, including the possible loss of customer trust.

When assessing appropriate technical measures, the following will be considered (amongst other measures):

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of portable data storage devices such as laptops;
- Security of local and wide area networks;
- Security of data in transit;
- Cloud storage of data;
- Cyber security;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate/relevant international security standards.

When assessing appropriate organisational measures the DPO will consider the following:

- The appropriate training levels throughout PA Housing;
- Supporting materials such as policies and procedures and reference material;
- Monitoring and checking measures that consider the reliability of employees;
- The inclusion of data protection confidentiality clauses in employment contracts;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;

- Appropriate controls on portable electronic devices outside of the workplace;
- Similar controls and checks on the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site.

These controls have been selected on the basis of identified risks to personal data and the potential for damage or distress to individuals whose data is being processed. Such risks and therefore matching controls will doubtless change over time.

Personal data shall not be transferred to a country or territory outside the European Union unless it has an adequate level of protection for the 'rights and freedoms' of data subjects.

UK DP legislation goes to some length to describe the controls that must be in place for the transfer of data outside the European Union area and a number of new concepts are introduced. See separate procedure – Transfer of personal data outside the EU area.

Appendix 3 – Data Subjects' rights – details

A3.1 Right of rectification

> An employee, tenant, former tenant or applicant for housing may challenge the information held by PA Housing on their particular file if they feel it to be incorrect and can provide evidence to support this.

The right of rectification under the GDPR (Article 16) entitles the data subject to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

A3.2 Erasure

Under the GDPR the rights of data subjects are extended to give individuals more protection and greater control over their personal information.

The right to erasure is also known as 'the right to be forgotten'. This enables an employee or resident to request the deletion or removal of personal data where there is no compelling reason for its continued processing by PA Housing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals only have a right to erasure where:

- the personal data is no longer necessary in relation to the purpose for which it was originally collected.
- where the individual withdraws consent.
- where the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- the personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- the personal data has to be erased in order to comply with a legal obligation.
- the personal data is processed in relation to the offer of information society services to a child.

PA Housing can refuse to deal with a request to erase where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to enable functions designed to protect the public to be achieved eg government or regulatory functions
- to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes;
- the exercise or defence of legal claims; or
- where the organisation has an overriding legitimate interest for continuing with the processing

A3.3 Restriction on processing

A data subject has the right to require a controller to stop processing his/her personal data. When processing is restricted, PA Housing is allowed to store the personal data, but not further process it.

PA Housing will be required to restrict the processing of personal data in the following circumstances:

- Where an individual (usually but not solely, employees or tenants) challenges the accuracy of the personal data, we must restrict processing until we have verified its accuracy.
- Where an individual has objected to the processing (where it was necessary for the purpose of legitimate interests), and we are considering whether our legitimate grounds override those of the individual.
- When processing is unlawful and the individual requests restriction instead of erasure.
- If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.
- If we have disclosed the personal data in question to third parties, we must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

We must inform individuals when we decide to remove the restriction giving the reasons why.

A3.4 Objection to processing

Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public tasks/exercise of official authority; direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

The only category relevant to PA Housing is where we process personal data for the purposes of our legitimate interests. In that case, where an individual (resident or employee) objects, we must stop processing the personal data unless:

- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

A3.5 Withdrawal of consent

An individual has the right to withdraw consent at any time. If the basis on which personal information is being processed is the consent of the individual, then that processing must stop. It may be that another reason for processing can be relied on such as legitimate interests.

In practice a withdrawal of consent is likely to be accompanied by a request to erase in which case PA Housing will need to rely on one of the other exceptions to erasure e.g. overriding legitimate interest.