Data Protection Policy

Document Control	
Document Title	Data Protection Policy
Author	Head of Business Support Services
Version	1.0
Release Date	May 2024
Next Review Date	May 2027
Document Type	Policy
Approved By	ARAC

POLICY SUMMARY

Please note that where we use EPIC within this policy, we refer to EPIC Housing Limited.

This Data Protection Policy outlines how EPIC processes the personal data, including, but not limited to, that of our tenants, housing applicants, suppliers, employees, workers, website users and other third parties and demonstrates how it complies with the principles and responsibilities of accountability set out in Article 5(2) of the UK GDPR.

This policy applies to all personal data we process regardless of the media on which that data is stored or processed.

1. APPLICABILITY

The Policy applies to all employees of EPIC regardless of whether they are permanent, contractor or temporary as well as Board Members and applies to home working for those who do this as part of their role. Volunteers, work placements and students as well as contractors, suppliers and agencies who have access to and handle personal data whilst carrying out work on behalf of EPIC are also covered.

2. INTRODUCTION

Article 9(2)(b) of the UK GDPR states that all data controllers should have an appropriate Data Protection Policy in place. We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. EPIC is exposed to potential fines, reputational damage and/or civil claims, for failure to comply with the provisions of the data protection laws. Individuals should also be mindful of the fact that they may also individually be committing a criminal offence.

All EPIC personnel, accessing or otherwise processing personal data controlled by EPIC have a responsibility for ensuring personal data is collected, stored and handled appropriately and must ensure that it is handled and processed in compliance with data protection law, this policy and the data protection principles.

EPIC collects and processes personal information about its tenants, board members, employees, employment applicants, housing applicants and suppliers (our stakeholders). Personal data is collected, processed, and where required, shared with third parties to effectively meet the requirements of the business and to ensure we are meeting the individual needs of our stakeholders.

To this end, EPIC is a Data Controller under the terms of the General Data Protection Regulation 2016 (GDPR). Where EPIC is providing services for other providers, we may also act as a Joint Controller or a Data Processor and assume the responsibilities relevant to those roles.

3. DATA PROTECTION DEFINITION AND PRINCIPLES

The GDPR, and the subsequent Data Protection Act 2018 (the UK law which implements the EU Regulation), laid down rules relating to the protection of living individuals with regard to the processing of personal data and rules relating to the free movement of personal data.

The GDPR protects the fundamental rights and freedoms of living individuals and in particular their right to the protection of personal data.

The Regulations are underpinned by the following principles, as per Article 5 of the UK GDPR, which state that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject (Lawfulness, Fairness and Transparency);
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Purpose Limitation);
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (Data Minimisation);
4. Accurate and, where necessary, kept up to date (Accuracy);
5. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data are processed (Storage Limitation);
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Security, Integrity and Confidentiality).

We have an overarching responsibility to demonstrate compliance with these principles throughout EPIC and in regard to all personal and special category data that we process. This policy has been developed following these principles and applies to personal data held in electronic and paper form and should also be applied to information shared verbally where there is a duty of confidentiality.

Definitions

For the purpose of this policy, the following definitions apply:

1. **Data Controller** – "the natural or legal person, public authority, agency or other body which, along or jointly with others, determines the purposes and means of the processing of personal data";
2. **Data Processor** – "the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller";
3. **Joint Controller** – "where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers";
4. **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 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";
5. **Special Category Data** – "any information 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, criminal activity, or data concerning a person's sex life or sexual orientation";
6. **Processing** – "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

Lawfulness, Fairness and Transparency

EPIC will only collect and process personal and special category data where we have a legitimate and lawful purpose to do so.

There are a number of lawful reasons for processing data contained within GDPR – and the following apply to EPIC:

a) Consent - The Data Subject has given their consent for their personal data to be processed;
b) Contract - Processing is necessary for EPIC to be able to deliver on the obligations of a contract (i.e. a tenancy agreement or an employment contract), or to be able to enter into a contract;
c) Legal obligation - Processing is necessary for EPIC to comply with another legal obligation that we are required to comply with (i.e. reporting a safeguarding incident, complying with a Police investigation, reporting benefit/tax/tenancy fraud);
d) Vital Interests - Processing is necessary for life-or-death reasons;
e) Legitimate Interests - Processing is connected to the legitimate interests of EPIC, except where such interests are overridden by the fundamental rights and freedoms of an individual. This could include, for example, processing information to support an individual to access employment or educational opportunities which would assist in our organisational aim to help people sustain their tenancies.

To lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9.

a) explicit consent from the data subject;
b) for the purposes of carrying out obligations or rights in the field of employment and social security and social protection law providing for appropriate safeguards for the fundamental rights and interests of the data subject;
c) to protect the data subject's vital interests;
d) to pursue legitimate activities by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on the condition that the processing relates solely to the members of the body or persons with regular contact and the data is not disclosed outside that body;
e) the personal data is manifestly made public by the data subject;
f) it is necessary for legal claims;
g) it is necessary for substantial public interest and measures to safeguard the rights of the data subject are provided;
h) it is necessary for preventative or occupational medicine, for the assessment of working capacity of the employee, medical diagnosis, provision of health or social care or treatment or the management of health or social care systems and services;
i) necessary for public interest in public health such as protecting against serious cross-border threats to health;
j) it is necessary for archiving in the public interest, scientific or historical research purposes or statistical purposes.

For EPIC, the most likely justification for processing a special category of personal data will be (a), (b) or (c) if this scenario occurs at all.

Purpose Limitation

EPIC will only collect and process data where there is a legitimate purpose for us to do so and will not use the data collected for any additional purposes without seeking consent from the Data Subject. Our published Privacy Policy provide transparent information to Data Subjects on our purposes and legal bases for processing personal data. All data processing activity is recorded in our Information Asset Register as required under Article 30 of the GDPR.

Data Minimisation

EPIC will not collect any personal data which is not necessary in connection to our relationship with the Data Subject. To this end, we are constantly reviewing our data collection methods, forms, etc. to review the contents and to strip out the collection of additional unnecessary data.

Accuracy
EPIC will review and update the personal data we hold about individuals regularly and during our routine transactions with individuals. We also place a responsibility on individual Data Subjects to inform us if their data is incorrect. EPIC colleagues can update their personal information within our HR System, and tenants can update their data by contacting any member of the EPIC team.

Storage Limitation
Article 5(1)(e) of the UK GDPR specifies that personal data should not be kept longer than required. EPIC is committed to upholding a proportionate and appropriate Data Retention Policy which ensures that personal and special category data is kept for no longer than is necessary. Where it is necessary to retain data for archiving purposes, anonymisation methods will be applied to further protect the rights and freedoms of the Data Subject. See the Data Retention Policy for more information.

Integrity and Confidentiality
EPIC has appropriate security measures in place to safeguard the personal and special category data that is processed, and it is the responsibility of all colleagues to ensure that the personal data which they have access to is kept securely and not disclosed to any unauthorised third parties. Article 5(1)(f) of the UK GDPR specifies that organisations should have appropriate measures of security in place to protect personal data.

Where appropriate, pseudonymisation or anonymisation of personal data should be applied to ensure the confidentiality of the data, and encryption tools should be used to protect personal information being transferred outside of EPIC by email. Further guidance on this can be obtained from the IT Technician.

Rights of the Data Subject
EPIC recognise that Data Subjects have the following rights under data protection legislation:

a) The right to transparent information and communication in relation to the personal and special category data that EPIC process (Article 13). We publish Privacy Statements which provide the following information to the Data Subject;
    - The contact details of the Data Controller
    - The contact details of the Data Protection Officer
    - The reasons why personal data is processed, including the legal basis for the processing
    - Details of any third parties whom data is shared with
    - Details of any international data transfers
    - Their rights under Data Protection legislation, including their right to complain with the Information Commissioner's Office
b) The right to access any personal or special category data processed by EPIC or our Data Processors (Article 15);
c) The right to rectification of inaccurate personal data (Article 16);
d) The right to erasure, otherwise known as the right to be forgotten, where the data processed by EPIC is no longer lawful or necessary, or was based on consent that has since been withdrawn (Article 17);
e) The right to restriction of processing where the accuracy or lawfulness of the data is contested (Article 18);
f) The right to data portability, i.e. the right to receive personal data in a structured, commonly used, machine-readable format (e.g. a CSV file) or to have that data transmitted to another Data Controller (Article 20);
g) The right to object to EPIC continuing to process their data where there is no longer a legitimate reason for us to do so (Article 21);

h) Rights related to automated decision-making and profiling where the automated decision could have a significant impact on them, and the associated right to request that a human reviews the decision made electronically (Article 22).

A Data Subject can express any of the above rights in any manner that they choose, but verification processes must be followed to ensure that data is not shared with the wrong person.

EPIC must respond, in full, to any expression of an individual's request within 1 calendar month. Where EPIC is unable to respond in full within 1 calendar month due to the size or complexity of the request, the Data Subject should be informed before the end of the first month of any additional time required.

Exemptions
The GDPR and the Data Protection Act 2018 contain a number of exemptions or restrictions which allow for EPIC to process information outside of the "usual" confines of the law. Such exemptions include, but are not restricted to:

- The prevention, detection or prosecution of criminal offences;
- Taxation, public health, or social security purposes;
- The protection of judicial independence and judicial proceedings;
- Matter of public security, national security, or defence;
- The safeguarding of children or individuals at risk.

Personal Data Breaches
A personal data breach means a breach of security resulting in the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, personal data.

If a data breach occurs, either accidentally or via malicious action, EPIC is obliged to investigate to determine the likely consequences of the breach, and the risks to the rights and freedoms of the Data Subject(s) to whom the data relates. Article 33 of the UK GDPR introduces a duty on all organisations to report certain types of data breach to the relevant supervisory authority. This must be done within 72 hours of becoming aware of the data breach, where feasible.

If a member of staff becomes aware of a data breach, then they should report it to the DPO immediately.

More information is contained within the Data Breach Procedure.

Information Asset Register
To satisfy Article 30 of the UK GDPR, EPIC holds an Information Asset Register which includes a description of the data collected, the legitimate reason for collecting this data, where the data is stored and who uses/has access to this. The Asset Register should be reviewed and amended should EPIC change the way that personal data is processed or processes new types of personal data.

Data Protection Impact Assessments
Under UK GDPR, EPIC has an obligation to consider the impact on data privacy during all processing activities. Where EPIC is considering the implementation or adoption of a new process or system that may result in an increased impact on privacy, we will carry out a Data Protection Impact Assessment to determine whether there are any alternative methods available which would minimise the risks to the rights and freedoms of individuals.

Where an impact assessment indicates that a new process or system poses a high risk to individuals that cannot be mitigated, EPIC will seek prior consultation with the Information Commissioner's Office

to gain their advice. More information is contained within the Data Protection Impact Assessment template and guidance.

Sharing Personal Data
We may be required to share data with third parties to deliver our services or to fulfil our legal obligations. We inform Data Subjects of the identity or category of these third parties at the point we collect their data within our published Privacy Statements. When engaging third parties in processing personal data, the terms of the data sharing are documented within a Data Sharing Agreement (a template for which is available).

We have clear processes in place to identify Data Subjects to prevent the unauthorised disclosure of data. This includes processes to verify the identity of any third-party advocates. Any requests for information from a third party are reviewed and verified before disclosing personal information.

Transfer of Personal Data
It may sometimes be necessary for EPIC to transfer personal information overseas. If the transfer involves data leaving the EU, EPIC will ensure the requirements of UK GDPR Chapter 5 are met.

EPIC transfers data to a small number of international data processors (e.g. Mailchimp) who are compliant with the rules above.

4. RESPONSIBILITIES

The roles and responsibilities of key stakeholders across EPIC are detailed below.

The Board is ultimately responsible for overseeing compliance with GDPR through oversight in relation to the obligations of the organisation as a Data Controller.

Audit and Risk Assurance Committee – have delegated authority from the Board to consider and approve GDPR policies.

CEO – has overall responsibility for ensuring the organisation complies with UK GDPR and DPA 2018 legislation through its policies and procedures.

Head of Business Support Services will act as the Data Protection Lead and provide data protection guidance and advice to colleagues and residents. They will act as the point of contact for the ICO and report annually to ARAC on our data protection management.

All managers are responsible for implementing this Policy and championing data protection within their teams.

All staff have a duty to maintain the security of personal information and special category data and are responsible for ensuring they adhere to this policy and escalate any potential data protection breaches to the Head of Governance as soon as possible.

Third-party organisations as Data Processors for EPIC will be expected to sign a Data Sharing Agreement to manage this relationship and the expectations associated with this function.

5. TRAINING

This policy forms part of the standard induction for all new employees, including agency workers, contractors, and Board members and will be read within the induction period. Staff will be referred to this policy when required and will be notified of changes when it is reviewed.

Periodic training will be provided on this policy as part of the annual learning and development plan. Further training may be provided if a data breach or near miss occurs and there may be communications to all staff around the breach/near miss for awareness/ training purposes.

6. DATA VALIDATION, REVIEW AND MONITORING

Overall responsibility for ensuring compliance with this policy lies with the CEO.

EPIC is committed to ensuring this policy complies with the requirements of GDPR and UK Data Protection legislation. This policy will be reviewed and updated upon such changes prior to the next review date.

7. EQUALITY AND DIVERSITY IMPLICATIONS

We are committed to ensuring and promoting equality of opportunity for all. We are opposed to discrimination on any grounds, including race, religion, gender, marital status, sexual orientation, disability, age, or any unjustifiable criteria. We are committed to developing a culture that values people from all sections of society and the contribution which each individual can make. We will ensure our approach to accessing properties is considerate to people's individual needs. We also adhere to the Equality Act 2010.

EPIC Housing recognises that some people experience disadvantage due to their socio-economic circumstances and will strive to ensure no person or groups of persons is treated with injustice due to their personal circumstances. EPIC Housing will also ensure that all services and actions are delivered within the context of current Human Rights legislation and will make sure the central principles of the Human Rights Act (1998) will be adhered to.

An Equality Impact Assessment has been completed on this policy that showed there was no detriment to any protected characteristic or group and no further development of the policy was needed.

It is noted that EPIC Housing collects and processes a range of personal and sensitive data about its tenants and other data subjects, allowing for a better understanding of their needs and the delivery of excellent service.

8. MONITORING / REVIEW

This policy will be reviewed every 3 years. A review may be conducted earlier if there are significant changes to either regulation, legislation, or EPIC's operating practices.

9. ASSOCIATED DOCUMENTS

- Privacy Notice
- Data Breach Procedure
- Disciplinary Procedure as detailed in the Staff Handbook
- EPIC's Code of Conduct
- Information Security and Acceptable Use Policy
- Document Retention Policy
- Data Protection Impact Assessment guidance

Version Control

Date of Review	Reviewer	Version Number	Changes	Date of Next Review	Approved By
May 2024	HoBSS	1.0	Rewrite of existing policy	May 2027	ARAC