DATA PROTECTION POLICY DOCUMENT

Under UK General Data Protection law (UK GDPR), Ekaya Housing Association (EHA or the Association) have a mandatory obligation to provide certain information to our employees, housing association contacts, residents, clients, and any other identifiable person whose personal data we might process.

Contained within this policy document are 3 important individual policies and procedures that are designed to provide clear guidance concerning our data processing activities and, importantly, the steps that can be taken by 'data subjects' to access personal data information that we may store about them within EHA.

Contained within this document are:

1. **Data Protection Policy and Procedure** – This is an internal-facing policy which sets out the principles and legal conditions that our data processors must satisfy when obtaining, handling, processing, transporting or storing personal data in the course of their jobs. This includes resident, supplier and employee data.

2. **Privacy Policy** – This is external-facing document informing those whose personal data we store, (primarily our employees and residents), about what we do with their personal data, how we handle it, store it, process it, who we share it with, how long we keep it for etc.

3. **Subject Access Request Policy and Procedure** – describes in detail the steps that a data subject, (e.g. an employee or resident), can take to request access to personal data that we hold. A Subject Access Request Form is provided at the end and can be used to formally make a Subject Access Request.

If you have any queries in relation to any of the information contained in this document, please contact the Data Protection Officer, the Director of Finance and Resources/Deputy CEO (DoR/DC).

Ekaya Data Protection Policy and Procedure

1 Introduction

1.1 This Policy sets out the obligations of Ekaya Housing Association (EHA or the Association), regarding data protection and the rights of customers both old and new and members of staff whether existing or not ("Data Subjects") in respect of their Personal Data under the Data Protection Act 2018 (DPA), UK General Data Protection Regulation ("UK GDPR") and the General Data Protection Regulation ("EU GDPR").

1.2 This Policy sets out the procedures that are to be followed when dealing with Personal Data. The procedures and principles set out herein must be followed at all times by the Association, its employees, agents, contractors, or other parties working on behalf of the Association. Any breach of this Policy may result in disciplinary action. This Policy does not form part of an employee's contract of employment and may be amended at any time.

1.3 The Association is committed not only to legal compliance, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all Personal Data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

1.4 EHA is registered with the Information Commissioners Office ("ICO") and supports the objectives of the UK GDPR: Registration Number: Z7146480.

2 Definitions and Interpretations of Terms Used In this Policy and Procedure

2.1 "**Personal Data**" is any information relating to an identified or identifiable natural person (a "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.

2.2 **Personal Data ("Special Categories")** covers racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, processing of genetic data, biometric data for the purpose of identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation, in the housing/employee context this could include matters such as:

2.2.1 medical issues and physical or mental health;

2.2.2 racial or ethnic origins information;

2.2.3 HIV/AIDS;

2.2.4 sexual orientation or any other information relating to a person's sexual life;

2.2.5 drugs/substance abuse;

2.2.6 religious beliefs or other beliefs of a similar nature;

2.2.7 child abuse;

2.2.8 domestic violence;

2.2.9 disability;

2.2.10 Trade union membership; and

2.2.11 political opinions.

2.3 "**Processing**" means obtaining, recording and keeping information as well as using it. The Association will correct, maintain, process and retain such personal data as is necessary for the proper administration of its business activities.

2.4 "**Data processing**" is 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, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.5 "**Data Subject**" means an individual who is the subject of personal data.

2.6 "**Data Controller**" means a person (alone, jointly or in common with other persons) who determines the purposes for which and the manner in which any personal data is processed.

2.7 "**Data Processor**" is the person who processes the data on behalf of the data controller.

2.8 "**Criminal offence data**" is data which relates to an individual's criminal convictions and offences.

2.9 "**Recipient**" means a person, to whom the data is disclosed, including any person to whom they are disclosed in the course of processing the data (i.e. employee or agent of data controller, data controller, data processor or employee or agent of data processor).

2.10 "**Third Party**" means any person, other than the data subject, the data controller and any other person authorised to process data.

2.11 "**Information Commissioner**" means the commissioner appointed under the UK GDPR and their appointed officers.

3 Staff

3.1 This Policy and Procedure will be issued to all employees.

3.2 Information will only be accessible to those staff who need it to carry out the Association's work.

3.3 Where a member of staff is unsure whether Personal Data is of Special Categories, advice should be sought from the Data Protection Officer, the Director of Finance and Resources/Deputy CEO (DoR/DC), or in their absence from their respective line manager or the Information Commissioner Office (ICO).

3.4 Interviews and conversations with employees and customers which involve discussion of special categories of Personal Data will always be carried out in private (i.e. away from public and open office areas).

4 Data Protection Principles

4.1 This Policy aims to ensure compliance with data protection laws. The UK GDPR sets out the following principles with which anyone handling Personal Data must comply. All Personal Data must be:

4.1.1 processed lawfully, fairly, and in a transparent manner in relation to the Data Subject;

4.1.2 collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes will not be considered to be incompatible with the initial purposes;

4.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

4.1.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

4.1.5 kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of the Data Subject;

4.1.6 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.

5 Lawful, Fair, and Transparent Data Processing

5.1 The Association seeks to ensure that Personal Data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the Data Subject. The UK GDPR states that processing of Personal Data will be lawful if at least one of the following applies:

5.1.1 the Data Subject has given consent to the processing of their Personal Data for one or more specific purposes;

5.1.2 processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;

5.1.3 processing is necessary for compliance with a legal obligation to which the Association is subject;

5.1.4 processing is necessary to protect the vital interests of the Data Subject or of another natural person;

5.1.5 processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Association;

5.1.6 processing is necessary for the purposes of the legitimate interests pursued by the Association or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

6 Data Subject Rights

6.1 Employees and residents have a right to view personal information about themselves and their family. They are entitled to know:

6.1.1 what data is held or otherwise processed about them;

6.1.2 the purposes of the processing;

6.1.3 the categories of personal data concerned;

6.1.4 the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

6.1.5 where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

6.1.6 the existence of the right to request from the controller (i.e. EHA) rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

6.1.7 the right to lodge a complaint with the ICO; and

6.1.8 where the personal data are not collected from the data subject, any available information as to their source.

6.2 Personal information – especially special categories of personal information – about employees and customers 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. Where appropriate, the Association sets up protocols to clarify how this operates in practice to ensure that only those people who have a need to know are able to access personal data of employees or residents.

7 Data Protection – Processes

7.1 EHA will only collect and process personal data where the following conditions have been met:

7.1.1 The data subject has given their consent; or

7.1.2 The processing is necessary for the performance of a contract with the data subject; or

7.1.3 The processing is necessary under legal obligation; or

7.1.4 The processing is necessary in order to protect the vital interests of the data subject; or

7.1.5 The processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

8 Data Security – Employees and Residents

8.1 Employees

8.1.1 The Association will not give out any personal information (e.g. title, salary, dates of employment, etc.) to banks, credit agencies or anyone requiring information, without written authorisation from the employee concerned unless permitted by this policy or otherwise by the UK GDPR. Employees who require data to be released should notify the Corporate Services Manager in writing.

8.1.2 Explicit consent is obtained from prospective employees who are asked to give their consent when they complete an application form, or it is obtained under the contract of employment.

8.1.3 Any internal information relating to special categories data will be marked as "private and confidential" and will only be passed to other sections of the Association if it is necessary for the purposes of pursuing legal action or considering disciplinary action against an employee.

8.1.4 All employee files will be kept in secure cabinets. Employee computer files will be given a security password so that staff can only gain access to employment records where they have a legitimate business need to do so.

8.2 Residents and Applicants

8.2.1 The Association's overall strategies will strive to achieve good practice as well as complying with its legal obligations under the UK GDPR to ensure that:

(a) where practicable, explicit consent from any resident will be obtained before personal information is passed on to outside bodies (see clause 9 – Requests for Information from Third Parties / Data Disclosures);

(b) the resident's explicit consent will be obtained before collecting and processing special categories of personal data. All relevant standard forms contain a clause to this effect. (NB: Ethnicity and gender information collected for the purposes of equal opportunities monitoring are excluded from these obligations);

(c) in both cases, (personal data and special categories 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;

(d) if another person, e.g. Social Worker, Support Worker or other person whom the resident has brought with them for support, is to be present, then the resident should be warned that the interview will involve discussion of personal and sensitive matters and their consent is obtained, (verbal consent will suffice providing it is precisely recorded) to the interview proceeding with the other person present;

(e) any internal information relating to special categories of personal data will be treated as private and confidential and will only be passed to other sections of the Association where:

(i) it is necessary for the provision of a service to the resident, e.g. in support of a resident's request for an urgent transfer; or

(ii) to protect the health and safety of staff, e.g. where the Association has information to indicate that a resident has aggressive or violent tendencies, and this information needs to be shared with staff visiting the resident by way of violent markers; or

(iii) legal action is being pursued or planned against a tenant, e.g. details of a tenant's mental health of disability will be passed to the Association's legal advisors in support of a possession action.

(f) any external correspondence about customers referring to special categories of personal data will be treated as "private and confidential" and the following will apply:

(i) Access to this information is strictly limited to a "need to know" basis.

(ii) If appropriate it should be explained that the association is unable to give full details in order to respect resident confidentiality, e.g. complaints of nuisance.

(iii) The Association will stipulate to its contractors and agents that they must take special care to maintain confidentiality and respect the privacy of residents and their homes.

8.2.2 Where a resident is known to have aggressive or violent tendencies and may pose a threat to visitors to their premises, the Association may disclose such information to contractors and agents who have been instructed to visit them. Disclosure of such information must be authorised by the appropriate departmental manager or Head of Service and any contractor or agent given such information shall be required to keep such information confidential. If the contractor is a company which provides regular contracting services to EHA, e.g. is appointed under a Framework, the contractor should also have entered into a Data Protection Agreement governing its use of personal data passed to it by EHA.

9 Requests for Information from Third Parties / Data Disclosures

9.1 Requests from outside organisations for information about employees or residents must be in writing unless there are good reasons for the matter to be dealt with orally, e.g. an urgent request from the police where somebody's health or safety is at risk. Such situations will be rare, and EHA will use its discretion to consider whether such disclosure would be appropriate in the circumstances.

9.2 EHA will ensure the safeguarding of its employees' and residents' rights is considered when approached by an outside agency with a request for disclosure.

9.3 The following may be organisations to which EHA has a legal obligation to disclose information:

9.3.1 The Inland Revenue

9.3.2 The Child Support Agency / Child Maintenance Service

9.3.3 The Benefits Agency

9.3.4 The Department of Work and Pensions

9.3.5 The Financial Conduct Authority

9.3.6 The Office for National Statistics

9.3.7 The Commission for Social Care Inspection

9.3.8 Criminal Records Bureau

9.3.9 The Regulator of Social Housing

9.3.10 Central and Local Government

9.3.11 Health and Safety Executive

9.3.12 Protection of Vulnerable Adults (POVA)

9.4 The Police

9.4.1 EHA intends to co-operate with the police in the prevention and detection of crime and the UK GDPR permits disclosure of information to the police for the prevention and detection of crime and the apprehension or prosecution of offenders. It also permits disclosure to the tax authorities in relation to the assessment or collection of tax or duties and disclosure to local authority benefit fraud teams in relation to the prevention and detection of benefit crime. In all these cases, disclosure can be made without the consent of the employee or resident.

9.4.2 In relation to residents, EHA may enter into or agree to local police protocols, which follow guidance from the ICO, (responsible for enforcement of the UK GDPR), governing the sharing of information between the police and EHA.

9.4.3 Under the terms of such protocols, EHA may obtain information from the police about residents for the purposes of investigating and/or preventing crime. Any information passing between the police and the Association is treated as confidential.

9.4.4 In certain circumstances EHA is also legally obliged to disclose personal information and consent is not required for the disclosure of information to the following:

(a) Local Authority in respect of Council Tax to enable the Authority to identify the person liable for Council Tax. EHA will normally require a written request.

(b) Benefits Agency and Housing Benefit Departments, if it suspects that an employee/resident is receiving benefits to which they are not entitled. For operating purposes, the Association will normally give the relevant information to assist the processing of an employee's or resident's claim.

(c) Electoral Officer is entitled under statute to disclosure of names and addresses of tenants of a Registered Provider.

9.5 Representatives

No information is given to tenants' representatives or advocates without the tenant's explicit written consent.

9.6 Data Requested by Research Organisations

EHA will inform residents and obtain their consent each time if it proposes to disclose personal data, in confidence, to another organisation for research purposes unless the information is anonymised or pseudonymised. (Pseudonymisation means that the personal data cannot be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to protect it.)

9.7 Social Services / Probation Service

9.7.1 Managers may decide whether or not to give relevant information, depending on the type of information required, the reason for asking for the information, and whether the resident's consent has been obtained.

9.7.2 If the resident's explicit consent has not been obtained, EHA should only make disclosure in order to fulfil its legitimate functions as a housing provider, e.g. in cases of anti-social behaviour or where it is necessary in order to protect the vital interests of the data subject to or another person.

9.8 Housing Ombudsman

The Housing Ombudsman is entitled to disclosure of a resident's file where they are investigating a complaint and any other information held by EHA which is relevant to the investigation (e.g. complaints file). This can include legally privileged correspondence passing between EHA and its solicitors. NB – in all other circumstances, privileged correspondence including notes of telephone advice and any other communications, e.g. e-mails between the Association and its solicitors are legally privileged information which must not be disclosed to residents or third parties even if held on tenancy files (see 10 – Access to Personal Information Refused). Before releasing any privileged information, this should be discussed with the relevant Head of Service.

9.9 Local Authorities

Staff should be aware that requests from local authorities for disclosure of personal information for "monitoring purposes" may not be permitted unless disclosure can be justified by reference to the Association's legal obligations or where the resident gives their explicit consent. Careful consideration should be given to requests for disclosure in each circumstance.

10 Right of Access to Personal Information

10.1 In addition to their rights under this policy all EHA's employees and tenants and anyone else in respect of whom personal data is processed have a right to ask the Association, for personal information held about them and this section details the information they are entitled to see.

10.2 The rights of our employees and residents are set out here for completeness, (see also EHA's Subject Access Request Procedure):

10.2.1 within one month of a written request a data subject is entitled to:

(a) be told whether personal data, of which they are the subject, is held in the Association's records, or otherwise processed by the Association;

(b) be given a description of the personal data, the purpose for which the data is being or may be processed and the persons or classes of persons to whom the data has been or may be disclosed to;

(c) have communicated to them in an intelligible form the information constituting the personal data held about them and any available detail as to the source of that information;

(d) be told the envisaged period for which the data will be stored or, if not possible, how it will be decided when it will be destroyed;

(e) be informed of their right to erasure of personal data; the right to object to processing; the right to rectification of data; to restriction on processing; and the right to object to processing;

(f) be informed of their right to complain to the ICO; and

(g) know of the existence of any automated decision-making, including profiling, and in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (this is not relevant to EHA currently as we do not currently engage in any form of profiling).

10.3 Residents are not entitled as of right to see property or maintenance files as these do not generally contain their personal data. If a resident is bringing a disrepair claim or other claim relating to the maintenance of their property, they may be entitled to disclosure of these files before commencing litigation under the Pre-Action Protocol for Housing Disrepair Cases (in the Civil Procedure Rules). However, they are not entitled to disclosure until sufficient particulars of their claim in an "Early Notification Letter" or a "Letter of Claim" have been provided.

10.4 If a resident or resident's representative (solicitor etc.) requests to see property records or maintenance files the request should be referred to the Head of Service and thereafter to EHA's legal advisers.

10.5 A resident is entitled to make a subject access request (SAR) under the UK GDPR. No fee is payable by the data subject unless a request is manifestly unfounded or excessive, particularly if it is repetitive, in which case we can charge a reasonable fee based on the administrative cost of providing the information. We may also charge a reasonable fee to comply with requests for further copies of the same information. The Government can set a limit on these fees. At present no fee limit has been set. A person making a subject access request on behalf of a resident must obtain and produce evidence of that resident's permission prior to any personal information being passed on.

10.6 Note: it is crucial before disclosing an employee's personnel file or resident's tenancy file that any information referred to in 11 – Access to Personal Information Refused – is removed before the employee or resident sees the file or obtains a copy.

11 Access to Personal Information Refused

11.1 EHA reserves the right to refuse the employee or resident access to information if:

11.1.1 it would identify another individual who has not consented to the disclosure. (Note: organisations are not covered by UK GDPR so information about them may be disclosed. However, to avoid any claims of breach of confidentiality, their consent should be sought and disclosure should only be made without their consent if it cannot reasonably be obtained and it is reasonable in all the circumstances to make disclosure);

11.1.2 it is legally privileged correspondence e.g. between EHA and its solicitors;

11.1.3 the data is held for management forecasting or management planning, and if the disclosure is likely to prejudice that activity e.g. information about plans to promote, transfer or make a worker redundant;

11.1.4 information containing details of EHA's intentions concerning negotiations with an employee is likely to prejudice those negotiations;

11.1.5 the information consists of a reference given or to be given in confidence by the employer for:

(a) the education, training or employment of the worker;

(b) the appointment of the worker to any office;

(c) the provision by the worker of any service. and

(d) the information is held for:

(i) the prevention of the detection of crime; and/or

(ii) the apprehension or prosecution of offenders; and/or

(iii) the assessment or collection of any tax or duty or any other imposition of a similar nature where access would be likely to prejudice any of the above matters;

(iv) the information was provided in confidence by a third party e.g. social workers, doctors, solicitors, local councils or the DWP;

(v) in the opinion of EHA or a health professional it would be likely to cause serious harm to the physical and/or mental health of a resident or another person; or

(vi) the information requested relates to non-personal details such as property records or maintenance details. The Association is only obliged to provide access to personal information about the resident and sometimes about their family.

12 Accuracy of Personal Information: Right of Rectification

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

12.2 The right of rectification 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.

13 Rights of Erasure, Restriction on/objection to Processing and Withdrawal of Consent

13.1 Erasure

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

13.1.2 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 EHA.

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

(a) the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;

(b) the individual withdraws consent;

(c) the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;

(d) the personal data was unlawfully processed (i.e. otherwise in breach of the UK GDPR);

(e) the personal data has to be erased in order to comply with a legal obligation; or

(f) the personal data is processed in relation to the offer of information by society services to a child.

13.1.4 The Association can refuse to deal with a request to erase where the personal data is processed for the following reasons:

(a) to exercise the right of freedom of expression and information;

(b) to enable functions designed to protect the public to be achieved e.g. government or regulatory functions;

(c) to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;

(d) for public health purposes in the public interest;

(e) for archiving purposes in the public interest, scientific research, historical research or statistical purposes;

(f) the exercise or defence of legal claims; or

(g) where the organisation has an overriding legitimate interest for continuing with the processing.

13.2 Restriction on Processing

13.2.1 A data subject has the right to require a controller to stop processing their personal data. When processing is restricted, EHA is allowed to store the personal data, but not further process it.

13.2.2 EHA will be required to restrict the processing of personal data in the following circumstances:

(a) Where an individual (usually, but not solely, employees or residents) challenges the accuracy of the personal data, we must restrict processing until we have verified its accuracy.

(b) 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.

(c) When processing is unlawful and the individual requests restriction instead of erasure.

(d) If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

(e) 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.

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

13.3 Objection to Processing

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

13.3.2 The only category relevant to EHA 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:

(a) we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or

(b) the processing is for the establishment, exercise or defence of legal claims.

13.4 Withdrawal of Consent

13.4.1 An individual has the right to withdraw consent at any time.

13.4.2 If the basis on which personal information is being processed is the consent of the individual, then that processing must stop.

13.4.3 It may be that another reason for processing can be legitimate interests.

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

14 Mergers and Acquisitions

14.1 Any information handed over to another organisation in connection with a prospective acquisition or merger will be anonymised. Personal information will be handed over only prior to the final merger or acquisition decision after securing assurances and a data protection agreement has been signed by the parties involved that it will be used solely for the evaluation of assets and liabilities.

14.2 Special categories of personal data will only be disclosed if one of the conditions set out in the UK GDPR has been satisfied.

14.3 Employees will be advised wherever practicable if their employment records are to be disclosed to another organisation before an acquisition or merger takes place.

15 Requirement to Notify Breaches

15.1 All Personal Data breaches must be reported immediately to the Data Protection Officer, the Director of Finance and Resources/Deputy CEO (DoR/DC).

15.2 If a Personal Data breach occurs and that breach is likely to result in a risk to the rights and freedoms of Data Subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer, the Director of Finance and Resources/Deputy CEO (DoR/DC), must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

15.3 In the event that a Personal Data breach is likely to result in a high risk (that is, a higher risk than that described under clause 15.2) to the rights and freedoms of Data Subjects, the Data Protection Officer, the Director of Finance and Resources/Deputy CEO (DoR/DC), must ensure that all affected Data Subjects are informed of the breach directly and without undue delay.

15.4 Data breach notifications will include the following information:

15.4.1 the categories and approximate number of Data Subjects concerned;

15.4.2 the categories and approximate number of Personal Data records concerned;

15.4.3 the name and contact details of the Association's Data Protection Officer (or other contact point where more information can be obtained);

15.4.4 the likely consequences of the breach;

15.4.5 details of the measures taken, or proposed to be taken, by the Association to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

15.5 The following are examples of data breaches:

15.5.1 access by an unauthorised third party;

15.5.2 deliberate or accidental action (or inaction) by a data controller or data processor;

15.5.3 sending personal data to an incorrect recipient;

15.5.4 computing devices containing personal data being lost or stolen;

15.5.5 alteration of personal data without permission; or

15.5.6 loss of availability of personal data.

16 When a Breach will be notified to the Individual

16.1 The Association will undertake to notify the individual whose data is the subject of a breach if there is a high risk to people's rights and freedoms. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

16.2 This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified. In all cases the breach must be reported to the Line Manager, the Data Protection Officer and the Corporate Services Manager/Company Secretary.

16.3 The following information will be provided when a breach is notified to the affected individuals:

16.3.1 A description of the nature of the breach.

16.3.2 The name and contact details of the appointed Data Protection Officer where more information can be obtained.

16.3.3 A description of the likely consequences of the personal data breach.

16.3.4 A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

17 Breach Detection Measures

We will implement measures to assist us in detecting a personal data breach. These measures will be monitored by our Data Protection Officer, the Director of Finance and Resources/Deputy CEO (DoR/DC).

18 Investigation into suspected Breach

In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by the Data Protection Officer, the Director of

Finance and Resources/Deputy CEO (DoR/DC), or in their absence, another member of the Senior Management Team (other than the person(s) being investigated), who will make a decision over whether the breach is required to be notified to the Information Commissioner. A decision will also be made over whether the breach is such that the individual(s) must also be notified.

19 Record of Breaches

The Association records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under UK GDPR. It records the facts relating to the breach, its effects and the remedial action taken.

20 Staff Training

20.1 All new staff must read and understand our policies on data protection as part of their induction.

20.2 All existing staff will receive periodic refresher training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

20.3 The nominated Data Protection Officer for the Association is trained appropriately in their role under the UK GDPR.

21 Monitoring, Review and Data Protection Compliance

21.1 The UK GDPR makes it obligatory for EHA to ensure that any personal information it holds on its employees, residents or any other person is accurate and kept up to date.

21.2 To ensure compliance EHA regularly asks its employees and residents to let them know if there have been any changes in personal circumstances so that personal information held on files can be updated.

21.3 No personal information will be kept for longer than is necessary but equally EHA will not delete information where there is a genuine business need to retain it.

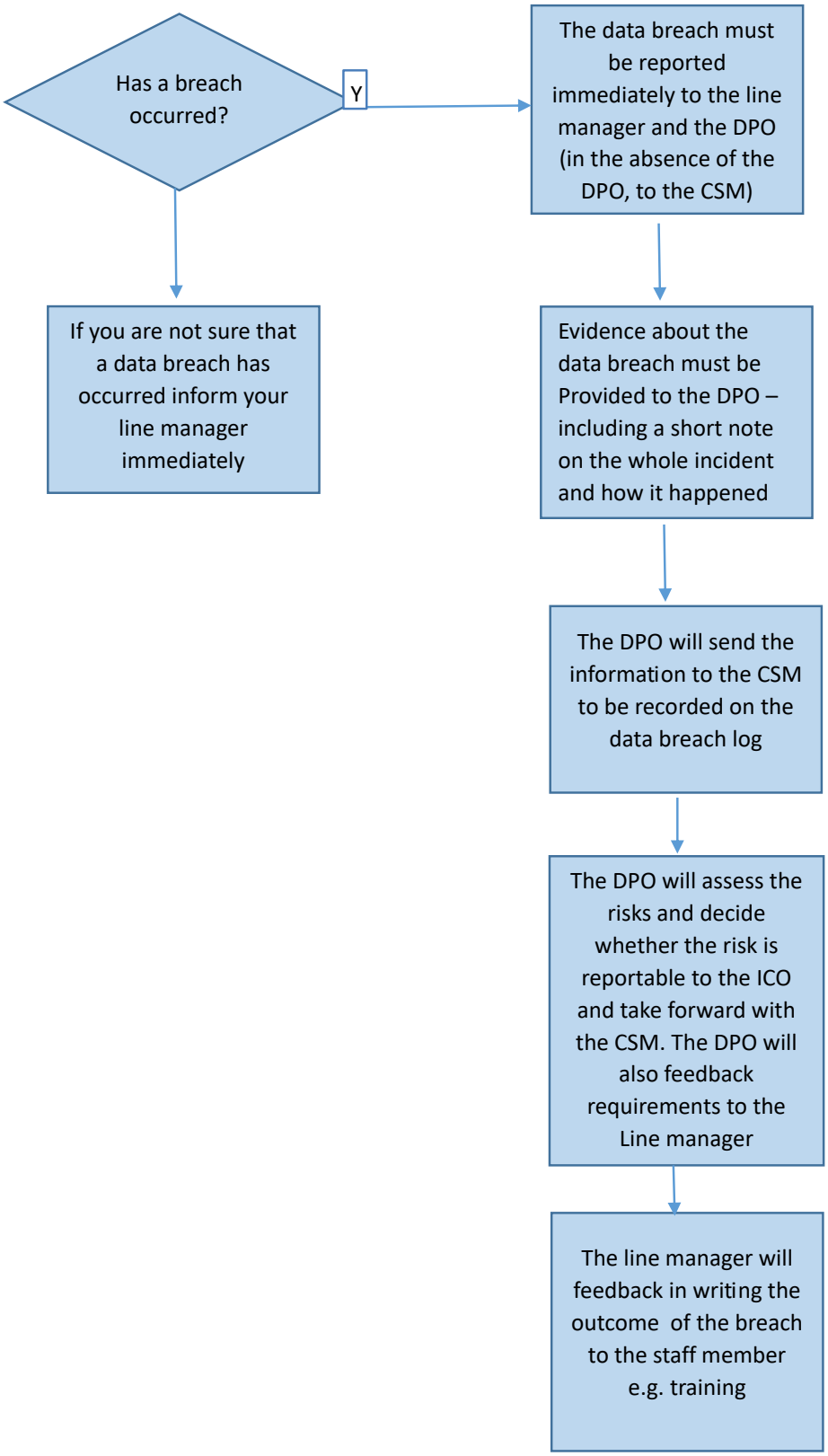
21.4 All written warnings will be removed from employees' personnel files once they have expired.

21.5 In addition, housing staff will ask residents in interview whether their circumstances have changed and check basic information about them and their household.

21.6 EHA has adopted National Housing Federation guidance on the retention of documents contained in the NHF Briefing Paper "Document Retention for Registered Social Landlords". The paper sets out recommended retention periods for documents including tenancy agreements and former residents' files. A copy is available from the Association's Intranet.

21.7 The Data Protection Officer, the Director of Finance and Resources/Deputy CEO (DoR/DC) will be responsible for UK GDPR compliance in the Association.

EKAYA HOUSING ASSOCIATION DATA BREACH PROCEDURE FLOWCHART



22 Policy Approval

Approval date: May 2023

Approved by: Policy and Performance / Audit and Risk Committees

Policy Owner: Corporate Services Manager

Staff consultation completed: March 2023

Next review date: March 2026

Where necessary, the Policy will be reviewed and updated prior to the review date, to reflect any legislative changes and good practice.

Ekaya Privacy Policy

1 Policy Statement

1.1 Ekaya Housing Association (EHA or the Association) respects the right to privacy of our Customers, Staff members, Board members, Contractors, Suppliers, Volunteers and other Stakeholders.

1.2 This Privacy Policy explains how we use any personal information we collect about you, and your rights to access and correct the personal information we hold about you.

1.3 We will collect and process your information and personal data in accordance with this Privacy Policy.

2 Data Protection Legislation

2.1 Our privacy policy complies with the General Data Protection Regulation (EU 2016/679) ("EU GDPR") as well as the retained EU law version of the EU GDPR (the "UK GDPR") and the Data Protection Act 2018 (together the "Data Protection Legislation") as at the date of our Privacy Policy.

2.2 **Data Controller:** Ekaya Housing Association (EHA), is the data controller and responsible for your personal data.

2.3 Where you provide us with your personal information in any of the ways described below, you agree that we may collect, store and use it:

2.3.1 in order to perform our contractual obligations to you;

2.3.2 based on our legitimate interests for processing your data (such as for internal administrative purposes, data analytics and benchmarking, direct marketing, maintaining automated back-up systems or for the detection or prevention of crime); or

2.3.3 based on your consent, which you may withdraw at any time, as described in our Privacy Policy.

3 What Personal Information We Collect and How We will use it

3.1 Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

3.2 We may collect, use, store and transfer the following different kinds of personal data about you:

3.2.1 Contact details including title, name, postal and email addresses, postcode, contact telephone numbers;

3.2.2 Your date of birth, place and country of birth and medical conditions, where applicable;

3.2.3 Demographic information;

3.2.4 Business information, such as employer details and job title;

3.2.5 Transaction information, including bank account details;

3.2.6 Customer communication preferences;

3.2.7 Customer feedback; and

3.2.8 Computer or device information (e.g. your IP address and operating system).

3.3 We may supplement the information that you provide to us with information from trusted third parties such as the banks, payroll bureau, contracted Consultants and/or government agencies (including Jobcentre Plus, HMRC, HMCTs, UKBA), for the purposes outlined in this Privacy Policy.

3.4 Where you instruct other third parties to act on your behalf, we may ask them to confirm the above information we hold about you (e.g. we may ask them to confirm, for identification purposes, your title, first name and surname, e-mail address, as we deem appropriate). You should always provide us with your express permission where you would want a third party to liaise with us on your behalf. We reserve the right to request to speak to you in person.

3.5 We may use your information for the following purposes:

3.5.1 Administration and management of your tenancy agreement, job application, contract of employment, Board membership or another contract with us, as applicable;

3.5.2 Processing transactions;

3.5.3 Administration and management of our residents', staff and/or Board member surveys, any competitions and prize draws etc. You should check the applicable terms and conditions of the survey, competition or prize draw for further information;

3.5.4 Sending you communications about our services. We may also send you service information communications (e.g. newsletters, annual reports, rent statements, invoices etc.). With your permission, we will keep you informed of news and update about the Association which we believe will be useful to you; and

3.5.5 Correspondence between us, including where you use our 'Contact us' form.

4 Providing us with information about others

If you provide us with personal information about someone else, you are responsible for ensuring that you comply with any obligation and consent obligations under applicable data protection laws in relation to such disclosure. In so far as required by applicable data protection

laws, you must ensure that you have provided the required notices and have obtained the individual's explicit consent to provide us with the information and that you explain to them how we collect, use, disclose and retain their personal information or direct them to read our Privacy Policy.

5 Sharing your personal information with third parties

5.1 We may disclose your personal information to, (in so far this is in line with applicable local data protection laws):

5.1.1 other service providers, contractors and other government agencies (aforementioned) for the purposes outlined above;

5.1.2 a Consultant who we have contracted to provide a service on our behalf; and/or any third party where we are under a legal duty to do so, or in order to enforce or protect any of our rights, property or safety, (or those of our Staff Members, Board Members, Contractors, Suppliers and other Stakeholders). This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

5.2 Where personal information is processed on our behalf by third parties, (such for the purposes of processing the payment of your rent, salaries and/or invoices, as applicable), we put measures in place to keep your information secure.

5.3 Our website contains links to other websites, mobile sites and apps. This Privacy Policy only applies to our on-line channels. When you link to other websites, mobile sites or apps we are not responsible or liable for them. You should read the privacy policies for those linked sites or apps before you submit any personal information to them. We are not responsible for the contents of external platforms.

6 Change of purpose

6.1 We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

6.2 If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

6.3 Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

7 Cookies

7.1 Our website uses cookies, which are small text files that contain small amounts of information that a website can send to, and store on, your computer or device through your browser. Cookies may be used by us to provide you with, for example, customised information from our website to make it more user-friendly.

7.2 By using our website, you agree to our Privacy Policy and consent to the use of cookies and similar technologies by us and our carefully selected third party partners as described in these policies.

8 Security

8.1 EHA takes the security of any personal information we hold very seriously. Where necessary, and in common with other websites and apps, we encrypt personal information provided to us to ensure it is neither accessible nor visible to anybody else when in transit between your computer and our servers.

8.2 In addition, our web servers are housed behind a secure firewall that prevents access to our databases by unauthorised users. All of our servers are housed in a secure environment with high levels of physical security.

8.3 However, the transmission of information via the internet is not completely secure. We cannot guarantee the security of your data transmitted to our site. Any transmission is at your risk. Once we have received your information, we will handle it in accordance with our usual practices.

8.4 In the event that you have chosen a password that enables you to access certain parts of our site, you are responsible for keeping this password confidential. We ask that you not to share a password with anyone.

9 Direct Marketing

9.1 We would like to keep you informed of any news that we believe would be useful to you, by post, phone, email, text and other electronic means.

9.2 If you have agreed to receive such communications you may opt out or change your marketing preferences at any time by contacting us at gdpr@ekaya.co.uk.

10 Access to and Amending Your Personal Information

10.1 We want to make sure that your personal information is accurate and up to date. You may ask us to correct or remove personal information you think is inaccurate by contacting us at gdpr@ekaya.co.uk.

10.2 You also have the right to request a copy of the personal information that we hold about you. To do so, please contact us at gdpr@ekaya.co.uk.

11 Data retention

11.1 We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

11.2 To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

11.3 In some circumstances we will anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

12 Your legal rights

12.1 Under certain circumstances, you have rights under the Data Protection Legislation in relation to your personal data, for example, you may be able to:

12.1.1 request access to your personal data;

12.1.2 request correction of your personal data;

12.1.3 request erasure of your personal data;

12.1.4 object to processing of your personal data;

12.1.5 request restriction of processing your personal data;

12.1.6 request transfer of your personal data; and

12.1.7 withdraw consent to processing of your data.

12.2 If you wish to exercise any of the rights set out above, please contact Data Protection Officer, the Director of Finance and Resources/Deputy CEO (DoR/DC). You will not have to pay a fee to access your personal data (or to exercise any of the other rights). If we hold any information about you which is incorrect or if there are any changes to your details, please let us know so that we can keep our records accurate and up to date. Please see Subject Access Request Procedure for further information.

13 Changes to our Privacy Policy

We keep our Privacy Policy under regular review, and we will place any updates on our website.

14 Contact Us

If you require further information or have any questions regarding this Privacy Policy, then please email us at gdpr@ekaya.co.uk, telephone us on 0207 091 1800 or write to us at: Ekaya Housing Association, 145 Stockwell Road, London SW9 9TN.

Ekaya Subject Access Request Policy

1 Introduction

1.1 Data subjects have certain rights in respect of their personal data and we respect and value those rights. These procedures provide a framework for responding to requests to exercise those rights and to ensure they are handled in accordance with applicable law (namely the Data Protection Act 2018 ("DPA") and the UK General Data Protection Regulation, ("UK GDPR")) and our internal procedures.

1.2 For the purposes of these procedures, "personal data" means any information relating to an identified or identifiable data subject. An identifiable data subject is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number or online identifier. “Processing” means any operation or set of operations that is performed on personal data, such as collection, use, storage, dissemination, and destruction.

1.3 These procedures apply to data subjects whose personal data we process, such as people who work for us and our Tenants.

1.4 The UK GDPR requires those who record and use personal information to be open about how the information is used and must make sure it is handled properly. The Act says that information about you must be:

1.4.1 fairly and lawfully processed;

1.4.2 processed for limited purposes;

1.4.3 adequate, relevant and not excessive;

1.4.4 accurate;

1.4.5 not kept for longer than necessary;

1.4.6 processed in line with your rights;

1.4.7 secure; and

1.4.8 not transferred to countries without adequate protection. By law, we are required to keep to these principles.

2 What information do you hold about me and why?

2.1 If you work for us, the information we store relates to your employment with us. Please contact the Data Protection Officer, the Director of Finance and Resources/Deputy CEO (DoR/DC), if you are an existing or ex-employee and would like to raise a subject access request.

2.2 If you are a Tenant, the information we hold on our records is usually related to your tenancy history. For example, this might include:

2.2.1 Names and dates of birth of people in your household.

2.2.2 Telephone numbers.

2.2.3 Rent payment history.

2.2.4 Information related to a transfer application, such as information on your health.

2.3 This list is not exhaustive, as we hold records of most contact that takes place between yourself and our offices. We keep this information so we can provide the services you need.

3 How do you protect my details?

3.1 It is our policy to ensure that:

3.1.1 information is only given to our staff and agencies on a need-to-know basis;

3.1.2 agencies with whom we share information observe our confidentiality policy;

3.1.3 all records are kept securely; and

3.1.4 interviews with residents will be carried out in private.

3.2 Personal information is treated as strictly confidential, unless you give consent, or the law permits it. For example, the law allows us to share information with Police, Benefits Agency and other landlords to prevent or deal with anti-social behaviour, crime and fraud.

4 How can I find out what information you hold about me?

4.1 You have a right, under the UK GDPR, to find out and to access the personal data we hold about you and to correct any mistakes. To do so, you should make a subject access request, and this policy sets out how you should make a request, and our actions upon receiving the request.

4.2 You can request a copy of all personal information we hold, including special categories of personal information. (Special categories of personal data cover racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation).

4.3 Although subject access requests may be made verbally, we would advise that a request may be dealt with more efficiently and effectively if it is made in writing. If you wish to make a request, please use the Subject Access Request form, (see Appendix 1).

4.4 Requests that are made directly by you should be accompanied by evidence of your identity. If this is not provided, we may contact you to ask that such evidence be forwarded before we comply with the request.

4.5 Requests made in relation to your data from a third party should be accompanied by evidence that the third party is able to act on your behalf. If this is not provided, we may contact the third party to ask that such evidence be forwarded before we comply with the request.

4.6 If you have made previous requests to view information, you will only be given information that has been added since your last request.

4.7 If you would like to authorise someone to access your personal data and act on your behalf, please complete a consent form in full and return to Ekaya Housing Association (EHA). If you wish to withdraw permission, you must notify us in writing.

4.8 If you telephone our offices to enquire about your rent account or personal matters related to your tenancy, you will be asked security questions to confirm your identity.

4.9 In responding to the request, we must provide you with the following information:

4.9.1 The purposes of the processing.

4.9.2 The categories of personal data concerned.

4.9.3 Special categories of personal data are defined.

4.9.4 The receipts or categories of receipt to whom the personal data have been or will be disclosed.

4.9.5 Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.

4.9.6 The existence of the right to request from EHA rectification or erasure of personal data or restriction of processing or to object to such processing.

4.9.7 The right to lodge a complaint with the ICO.

4.9.8 Where the personal data is not collected from the data subject, any available information as to their source.

4.9.9 The existence of automated decision-making, including profiling, and in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

5 Timescales

Usually, we will comply with your request without delay and at the latest within one month of your request. Where requests are complex or numerous, we may contact you to inform you that an extension of time is required. We can extend the period of compliance by a further two months, which is the maximum extension period.

6 Fee

6.1 We will normally comply with your request at no cost. However, if the request is manifestly unfounded or excessive, or if it is repetitive, we may contact you requesting a reasonable fee,

based on the administrative cost of providing the information. This fee must be paid in order for us to comply with the request. The fee will be determined at the relevant time and will be set at a level which is reasonable in the circumstances.

6.2 In addition, we may also charge a reasonable fee if you request further copies of the same information.

7 What will you send to me?

7.1 We will send you the information you have requested within the timescales specified in clause 5 above.

7.2 When you make a subject access request, you will be informed of:

7.2.1 whether or not your data is processed and the reasons for the processing of your data;

7.2.2 the categories of personal data concerning you;

7.2.3 where your data has been collected from if it was not collected from you;

7.2.4 anyone who your personal data has been disclosed to or will be disclosed to, including anyone outside of the UK and the safeguards utilised to ensure data security;

7.2.5 how long your data is kept for (or how that period is decided);

7.2.6 your rights in relation to data rectification, erasure, restriction of and objection to processing;

7.2.7 your right to complain to the Information Commissioner if you are of the opinion that your rights have been infringed; and

7.2.8 the reasoning behind any automated decisions taken about you.

7.3 You may be invited to view the data at one of our offices if we are unable to send it.

7.4 Please note that your right to see certain information may be limited. For example, if it may affect a police investigation of criminal prosecution then we are not permitted to disclose this information to you.

8 Circumstances in which your request may be refused

8.1 We may refuse to deal with your subject access request if it is manifestly unfounded or excessive, or if it is repetitive. Where it is our decision to refuse your request, we will contact you without undue delay, and at the latest within one month of receipt, to inform you of this and to provide an explanation. You will be informed of your right to complain to the ICO and to a judicial remedy.

8.2 We may also refuse to deal with your request, or part of it, because of the types of information requested. For example, information which is subject to legal privilege or relates to management planning is not required to be disclosed. Where this is the case, we will inform

you that your request cannot be complied with, and an explanation of the reason will be provided.

9 Can I appeal?

9.1 If you feel our records are inaccurate, you can write to us asking for them to be amended.

9.2 If you feel we have unfairly withheld information or unfairly refused to amend our records, you can make a complaint to the Data Protection Officer, the Director of Finance and Resources/Deputy CEO (DoR/DC), using our standard complaints procedure. Alternatively, you can contact the Information Commissioners Office.

Ekaya Subject Access Request Procedure

1 Procedure

1.1 Those who are entitled to make requests for data are those persons for whom we keep hard copy or computerised records that include personal data, including special categories of personal information. These are likely to be:

1.1.1 past and present employees, (all enquiries should be directed to the Data Protection Officer, the Director of Finance and Resources/Deputy CEO (DoR/DC), in the first instance); and

1.1.2 tenants, members of the household over 18, former tenants and persons referred to us for housing by our referral agencies.

1.2 Requests may be made in writing using the Subject Access Request Form (Appendix 1).

1.3 All requests from current and former tenants must be passed to the relevant Tenancy Services Officer. Request from referrals must be passed to the Tenancy Services Officer who will forward a Subject Access Request Form to the referral with Section B completed.

1.4 The identity of the person requesting the information must be proved. It is anticipated that in most cases the signature can be verified against the records we hold. In cases where there is doubt as to the identity, or there is no record available, further proof must be sought.

1.5 Examples of satisfactory proof include:

Personal Identity	**Address Verification**
Current valid (signed) full UK passport	Recent utility bill – Gas, Electricity, Water, Telephone (not mobile phones)
Current valid (signed) overseas passport	Mortgage Statement or Mortgage Redemption Statement
Current valid EEA member state ID card	Council Tax Bill
Current Residency Permit Issued by Home Office	Current Full UK Driving Licence (paper document)
Current Full UK Driving Licence	Current Full UK/EU Photo Card Driving Licence
Current Full UK/EU Photo Card Driving Licence	House or motor insurance certificate
Current state pension book/notification letter	Current state pension book/notification letter
Current Benefits Agency Book/letter	Current local rent card, Rent book authority or Tenancy Agreement

Current year's Inland Revenue Tax Code Notification	Bank/Building, Society/Credit Union Statement or Passbook
	Solicitor's letter confirming completion of house purchase or land registration
	Credit card statement
Or a combination of these	

1.6 NB: There are no rules for this. Use your judgement and if in doubt seek advice from the Data Protection Officer, the Director of Finance and Resources/Deputy CEO (DoR/DC), or a Head of Service.

1.7 The Housing Officer must confirm in writing that the identity is proved, and the 'Office Use Section' completed. If the person requesting has used the standard letter then the bottom of this letter should be completed. If the subject has written their own letter then the bottom of the Subject Access Request Sheet should be completed instead. Once the identity is proved the papers should be passed to the person who will obtain the printouts.

1.8 The person obtaining the printouts will print one copy of all the data held about the person and their household. This will include any screen with details in the Tenant's Register or Tenancy Details. Where any information is entered in the form of a code the literal interpretation of the code should be clearly entered next to the code or identified by a key written elsewhere on the printout.

1.9 The printout should be returned to the Housing Officer at least one week before the reply is due to be sent. The covering letter, and the printouts should be posted to the tenant by recorded delivery within one month of the date of the original request, or of proof of identity being determined.

1.10 A copy of the letter and the printouts must be kept for our records. The Tenancy Services Officer files all the papers in the relevant tenant or referral files.

1.11 If the request was made by electronic means, the information should be provided electronically unless the data subject agrees otherwise.

2 Request for Correction or Deletion of Data

2.1 Any request for data that is held on our computer files to be corrected or deleted should be made in writing, dated and signed by the person concerned. This letter should be passed to the Housing Services Manager as appropriate.

2.2 The Housing Services Manager will check that the details to be corrected or deleted are those which can be changed. Examples are dates of birth, spellings of names, members of household, etc. Requests cannot be made to change information such as nominating agency, date Notice of Seeking Possession served, etc., unless there has actually been an error on the Association's part.

2.3 NB: If a tenant is disputing information held on the rent account it may not be possible to simply do a correction. This should be treated as a normal dispute over the arrears. If any adjustment is made on the Association's part, it will show as an adjustment to the tenant's account.

2.4 To correct personal data the Housing Services Manager will complete the appropriate parts of the Tenants Register Amendment form as appropriate. A printout should be made.

2.5 A second explanatory letter should be completed and photocopied. This should then be sent by Recorded Delivery to the person requesting the corrections as confirmation that they have been made. The copy of the letter and printout should be placed in the relevant file.

Ekaya Subject Access Request Form

Please complete and return this form to:	Ekaya Housing Association Ltd 145 Stockwell Road, London SW9 9TN Tel: 020 709 11 800

About this form

You may use this form if you wish to make a formal request to view personal information held about you by Ekaya Housing Association (EHA). All day-to-day enquiries (e.g. maintenance request, tenancy and rent queries), can be handled by EHA via the telephone number above.

For further details on making a Subject Access Request, please refer to the additional information on page 3 of this form.

Section A: Your Details (person making the request)		
Full Name:	Tenancy Ref:	
Address:		
	Postcode:	
Home Phone Number:	Mobile Number:	
Email:		
Are you:		
A current or former member of staff? Yes/No	A current or former EHA resident? Yes/No	Another individual (please tell us about your connection with EHA) Yes/No

Section B: The Data Subject		
The Data Subject is the person whose personal information you are requesting		
Are you the Data Subject?	Yes (Please go to Section C)	No (Please continue below)
If no, you must enclose written authority from the Data Subject to show that you are acting on their behalf, (see page 3 of this form). Please also describe your relationship to the Data Subject, which leads you to make the request on their behalf.		
Details of the Data Subject (if different to Section A)		
Full Name:	Tenancy Ref:	
Address:		
	Postcode:	
Home Phone Number:	Mobile Number:	
Email:		
Are you:		
A current or former member of staff? Yes/No	A current or former EHA resident? Yes/No	Another individual (please tell us about your connection with EHA) Yes/No

Section C: Personal Information You Are Requesting
Please use this section to tell us what Personal Data you would like to see. 'Personal data' means information relating to the Data Subject as an individual, covering things like their tenancy details and rent payments and includes special categories of personal information. It does not routinely cover information relating to maintenance orders or property condition, as these do not usually contain personal data. Please be specific as this will speed up our response.

Please indicate under which service(s) your request falls and what data / documents you would like to see.

Service	**Information / documents you would like to request**
Lettings and transfers	
Anti-social behaviour	
Collection of rent or service charge	
Setting of rent or service charge	
Customer relations (a complaint that you have made)	
Tenancy	
Other (please specify)	

Please indicate under which service(s) your request falls and what data / document(s) you would like to see. Note: If CCTV search is required, please specify date(s), time(s) and location:

Section D: Declaration	
I certify that the information given on this form is true. I understand that it may be necessary to confirm my/the data Subject's identity and provide more detailed information before disclosing any data.	
Signed:	
Name (please print):	Date:
Please return the completed form to: Ekaya Housing Association Ltd, 145 Stockwell Road, London SW9 9TN	

Office Use Only
Date request received:
Date request completed:
Notes:

Additional Information
Please note: Information can only be sent to current EHA residents at the listed address. Non-EHA residents and representatives must produce evidence of their identity and address before viewing information (Fig 1.0 below). The requestor will be contacted to discuss what the most suitable option is for viewing data. EHA reserves the right to obscure or suppress information that relates to third parties (under the terms of UK GDPR). Personal information collected on this form is required to enable the Subject Access Request to be processed, and will only be used in connection with this request.

Fig 1.0 Table of acceptable forms of identification to confirm identity and address	
Personal Identity	**Address Verification**
Current valid (signed) full UK passport	Recent utility bill – Gas, Electricity, Water, Telephone (not mobile phones)
Current valid (signed) overseas passport	Mortgage Statement or Mortgage Redemption Statement
Current valid EEA member state ID card	Council Tax Bill
Current Residency Permit Issued by Home Office	Current Full UK Driving Licence (paper document)

Current Full UK Driving Licence	Current Full UK/EU Photo Card Driving Licence
Current Full UK/EU Photo Card Driving Licence	House or motor insurance certificate
Current state pension book/notification letter	Current state pension book/notification letter
Current Benefits Agency Book/letter	Current local rent card, Rent book authority or Tenancy Agreement
Current year's Inland Revenue Tax Code Notification	Bank/Building, Society/Credit Union Statement or Passbook
	Solicitor's letter confirming completion of house purchase or land registration
	Credit card statement
Or a combination of these	