Data protection policy Abbey Rentals (Eynsham) Ltd

Context and Overview

Key details

- Policy prepared by: Cindy Creasey
- Approved by Directors on:
- Policy became operational on:
- Next review date:
- Reviewed
- Next Review

Introduction

Abbey Rentals (Eynsham) Ltd may process information you provide including your customer details e.g name, phone numbers, email , residential address, and any transactional data including bank account details. All such data is treated as personal data for the purpose of the General Data Protection Regulation (GDPR) 2018. Our aim when collecting this type of information is to serve you better, so we will not sell your information to any third parties.

Abbey Rentals (Eynsham) Ltd needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards-and to comply with the GDPR.

Why this policy exists

This data protection policy ensures Abbey Rentals (Eynsham) Ltd:

- Complies with GDPR and follow good practice
- Protects the right of staff, customers and partners
- Is open about how it stores and processes individuals data
- Protects itself from the risks of a data breach

GDPR law

GDPR 2018 describes how organisation including Abbey Rentals (Eynsham) Ltd must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal Information must be collected under one of the six Lawful Basis's and used fairly, stored safely and not disclosed unlawfully.

Determining lawful basis to collect and hold

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

“a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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 shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

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

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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.”

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone’s life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

People, risk and responsibilities

Policy scope

This policy applies to:

- The head offices of Abbey Rentals (Eynsham) Ltd
- All branches of Abbey Rentals (Eynsham) Ltd
- All staff and volunteers of Abbey Rentals (Eynsham) Ltd
- All contractors, suppliers and other people working on behalf of Abbey Rentals (Eynsham) Ltd

What information does the GDPR apply to?

- **Personal data**

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data"
The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.
Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Data Protection risks

This policy helps to protect Abbey Rentals (Eynsham) Ltd from some very real data security risks, including:

- **Breaches of Confidentiality**. For instance, information being given out inappropriately.
- **Failing to Offer Choice**. For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage**. For instance, the company could suffer if hackers successfully gained access to sensitive data.
- A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Responsibilities

Everyone who works for or with Abbey Rentals (Eynsham) Ltd has responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that Abbey Rentals (Eynsham) Ltd meets it's legal obligations.
- **Jane Dodds** is responsible for:
  - Keeping the board updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection training and advice for people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data Abbey Rentals (Eynsham) Ltd holds about them (also called 'subject access requests').
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

- Approving any data protection statements attached to communications such as emails and letters. Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work.**
- Data **should not be shared informally.** When access to confidential information is required, employees can request it from their line managers.
- **Abbey Rentals (Eynsham)Ltd will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.**
- Employees should make sure paper and printouts are **not left where unauthorised people could see them,** like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

- **If you are a Landlord or tenant** we will retain your data for a maximum of 6 year after your tenancy or business with us has ended. This is in accordance with current legal requirments.
- When data is **stored electronically,** it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD, DVD USB or removable disks), these will be kept secure and if used to store or transport confidential data then they will be encrypted to prevent unauthorised access.
- should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers,** and should only be uploaded to an **approved cloud computing services.**
- Servers containing personal data should be **sited in a location**, away from general office space.
- Data should be **backed up frequently.** Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall.**
- Only **authorised employees** will be able to access company networks**, guest** access will be maintained separately.

Data use

Personal data is of no value to Abbey Rental (Eynsham) Ltd unless the business can make use of it. Should you go ahead with a property application your data will need to be passed onto a third party referencing company, consent will be asked for before going ahead with this. However, it is when personal data is accessed and used that it can be at the greater risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally.** In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contracts.
- Personal data should **never be transferred outside the European Economic Area.**
- Employees **should not save copies of personal data to their own computer.** Always access and update the central copy of any data.

Data accuracy

The law requires Abbey Rentals (Eynsham)Ltd to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Abbey Rentals (Eynsham)Ltd should put into ensuring it's accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary.** Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- Abbey Rentals (Eynsham) Ltd will make it **easy for data subjects to update the information** Abbey Rentals (Eynsham) Ltd holds about them. For instance, via the company website.
- Data should be **updated as inaccuracies are discovered.** For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Individual Rights

Under GDPR individuals have seven rights to their data, should a data subject require this information or want to evoke one of their right's this will need to be put in writing to Data Protection Officer Jane Dodds jmd@abbey-rentals.co.uk

Right to be informed
Right of access
Right rectification
Right to erasure
Right to restrict processing
Right to data portability
Right to object

Subject access requests

The GDPR sets out the information that you should supply and when individuals should be informed.

The information you supply is determined by whether or not you obtained the personal data directly from individuals.

The information you supply about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

You can charge a fee, however you can only charge a reasonable fee if it's excessive, & repetitive, the fee must be based on an administrative cost of providing information.

Information must be given without delay and within one month, this can be extended to two months were requests are complex or numerous, if this is the case you must inform recipient or why the extension is necessary.

How should the information be provided?

You must verify the identity of the person making the request, using 'reasonable means'.

If the request is made electronically, you should provide the information in a commonly used electronic format.

Subject requests from individuals should be made by email, addressed to the data controller at jmd@abbey-rentals.co.uk the data controller can supply a standard request form, although individuals do not have to use it.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Providing Information

Abbey Rentals (Eynsham) Ltd has a consent form that will need to be signed by an individual to ensure that they are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. This is available on request, a version of this statement is also available on the company's website.