Canning & Culshaw Property LTD (trading as BlueKeyLiving)
Data Protection Policy - Reviewed October 2019

1. Introduction

Canning & Culshaw Property LTD (trading as BlueKeyLiving) ('the business', 'we') collects and uses certain types of personal information about tenants, investors and other individuals who come into contact with the business in order to provide accomodation, investments and other associated functions. The business may be required by law to collect and use certain types of information to comply with statutory obligations related to tenancy agreements and right to rent. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (GDPR) and other related legislation.

The GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured is some way that is searchable on the basis of a specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed every 2 years.

2. Personal Data

'Personal data' is information that identifies an individual, and includes information that would identify an individual to the person whom it is disclosed because of any special knowledge that they have or can obtain. A subset of personal data is known as 'special category personal data'. This special category data is information that relates to:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health
- An individual's sex life or sexual orientation
- Genetic or biometric data for the purpose of uniquely identifying a natural person

Special category information is given special protection, and addition safeguards apply if this information is to be collected and used.

Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.
The business does not intend to seek or hold sensitive personal data except where the business has been notified of the information, or it comes to the business' attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Data subjects are under no obligation to disclose their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

3. The Data Protection Principles

The six data protection principles as laid down in the GDPR are followed at all times:

- Personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;
- Personal data shall be collected for specific, explicit and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
- Personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;
- Personal data shall be accurate and, where necessary, kept up to date;
- Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;
- Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

In addition to this, the business is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law. The business is committed to complying with the Data Protection principles at all times. This means that we will;

- Be responsible for checking the quality and accuracy of the information
- Regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy
- Ensure that when information is authorised for disposal it is done appropriately
- Ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer systems, and follow the relevant security policy requirements at all times
- Share personal information with others only when it is necessary and legally appropriate to do so

- Set out clear procedures for responding to requests for access to personal information known as ‘subject access requests’
- Report any breaches of the GDPR in accordance with the procedure outlined in Section 13.

4. Lawful Bases for Processing Data

- The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given
- The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering a contract with the individual, at their request
- The processing is necessary for the performance of a legal obligation to which we are subject
- The processing is necessary to protect the vital interests of the individual or another
- The processing is necessary for a legitimate interest of the business or that of a third party, except where this interest if overridden by the rights and freedoms of the individual concerned

5. Use of Personal Data by Canning & Culshaw Property LTD

We hold personal data on tenants, staff, investors and other individuals who come into contact with the business. In each case, the personal data must be treated in accordance with the data protection principles as outlined above.

Tenants

The personal data held regarding tenants includes; name, address, contract details (assured shorthold tenancy agreements (ASTs), phone number, email address, payment history (rent), nationality/visa status (right to rent), other relevant information and CCTV footage where in use.

The data is used in order to support our tenants, provide maintenance and safety certificates, onboard new tenants and manage our tenancies and properties.

We may also receive data about tenants from third parties, such as other landlords (e.g. referencing).

Staff

Personal data held about staff will include contact details, employment history, information relating to career progression, bank details (for payment of salary), photographs and videos.

The data is used to comply with legal obligations placed on the business in relation to employment. Personal data will be used when giving references.

Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction.

Other Individuals

The business may hold personal information in relation to other individuals who have contact with the business, such as agents, maintenance, other landlords and investors. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.

6. Security of Personal Data

The business will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this policy and their duties under GDPR. The business will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

7. The Data Controller

The business processes personal information relating tenants and staff, and is therefore a data controller. The directors have responsibility of data controller.

The business is registered as a data controller with the Information Commissioner's Office (ICO) and renews this registration annually.

8. Roles and Responsibilities

The directors have overall responsibility for ensuring the business complies with its obligations under the General Data Protection Regulation.

Day-to-day responsibilities rest with the Data Protection Officer, or other director in the Data Protection Officer's absence. The Data Protection Officer will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the business of any changes to their personal data, such as a change of address.

9. Subject Access Requests

Anybody who makes a request to see any personal information held about them by the business is making a subject access request. All information relating to the individual should be considered for disclosure.

All requests should be forwarded to the Data Protection Officer upon receipt, and must be dealt with in full without delay and at the latest within one month of receipt.

Any individual with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the business must have written evidence that the individual has authorised the person to make the application and the Data Protection Officer must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

Access to records will be refused in instances where an exemption applies, for example, where information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offences.

A subject access request must be made in writing. The business may ask for any further information reasonably required to locate the information.

An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

All files must be reviewed by the Data Protection Officer before any disclosure takes place. Access will not be granted before this review has taken place.

Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more practicable. A copy of the full document and the altered document should be retained, along with an explanation as to why the document was altered.

Exemption to access data by subjects

Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

There are other exemptions from the right of subject access. If we intend to apply any of them to a request then we will explain which exemption is being applied and why.

To make a request for your personal information please complete the Subject Access Request Form, taking note of the guidance for completion.

10. Other Rights of Individuals

The business has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the business will comply with the rights to;

- Object to Processing;
- Rectification;
- Erasure; and
- Data Portability

Right to object to processing

An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest.

Where such an objection is made, it must be forwarded to the Data Protection Officer upon receipt, and the Data Protection Officer will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

The Data Protection Officer shall be responsible for notifying the individual of the outcome of their assessment.

Right to rectification

An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be forwarded to the Data Protection Officer upon receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be

given the option of a review or an appeal direct to the information commissioner. An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

- Where the personal data is no longer necessary for the purpose for which it was collected and processed;
- Where consent is withdrawn and there is no other legal basis for the processing;
- Where an objection has been raised under the right to object, and found to be legitimate;
- Where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
- Where there is a legal obligation on the business to delete

The Data Protection Officer will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and/or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

In the following circumstances, processing of an individual's personal data may be restricted:

- Where the accuracy of the data has been contested, during the period when the business is attempting to verify the accuracy of the data;
- Where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
- Where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;
- Where there has been an objection made, pending the outcome of any decision.

Right to portability

If an individual wants to send their personal data to another organisation they have a right to request that the business provides their information in a structured, commonly used, and machine readable format.

As this right is limited to situations where the business is processing the information on the basis of consent or performance of a contract (such as an AST), the situations in which this right can be exercised will be limited. If a request for this is made, it should be forwarded to the Data

Protection Officer upon receipt, and the Data Protection Officer will review and revert as necessary.

11. Breach of any Requirement of the GDPR

Any and all breaches of the GDPR, including a breach of any of the data protections principles shall be reported as soon as it is discovered, to the Data Protection Officer.
Once notified, the Data Protection Officer shall assess:

- The extent of the breach;
- The risks to the data subjects as a consequence of the breach;
- Any security measures in place that will protect the information;
- Any measures that can be taken immediately to mitigate the risk to the individuals.

Unless the Data Protection Officer concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the business, unless a delay can be justified.
The information Commissioner shall be told:

- Details of the breach, including the volume of data as risk, and the number and categories of data subjects;
- The contact point for any enquiries (usually the Data Protection Officer);
- The likely consequences of the breach;
- Measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Data Protection Officer shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.
Data subjects shall be told;

- The nature of the breach;
- Who to contact with any questions;
- Measures taken to mitigate any risks.

The Data Protection Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed and a decision made about implementation of those recommendations.

12. IT Policy

This ensures staff understand what is acceptable when using IT equipment, software and data in the business. This document is part of staff member's mandatory data protection training.

13. Disposal of records

Inaccurate or out of date records will be disposed of securely, where we cannot or do not need to rectify or update it. The business shall shred or incinerate paper-based records, and overwrite or delete electronic files.
Personal data that is no longer needed will be disposed of securely.