Ross Sales & Lettings

PRIVACY POLICY

Contents

1. Introduction

Ross Sales & Lettings (“we” or “us”) is committed to ensuring the secure and safe management of data held by us in relation to customers, staff and other individuals. Our staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals’ data in accordance with the procedures outlined in this policy and documentation referred to herein.

We need to gather and use certain information about individuals. These can include customers (tenants, landlord clients etc.), employees and other individuals that we have a contractual relationship with. We manage a significant amount of data, from a variety of sources. This data contains “personal data” and “sensitive personal data” (known as “special categories of personal data” under the GDPR).

This policy sets out our duties in processing that data, and the purpose of this policy is to set out the procedures for the management of such data.

2. Legislation

It is a legal requirement that we process data correctly; we must collect, handle and store personal information in accordance with the relevant legislation.

The relevant legislation in relation to the processing of data is:

(a) the General Data Protection Regulation (EU) 2016/679 (the GDPR);

(b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and

(c) any legislation that, in respect of the United Kingdom (UK), replaces, or enacts into UK domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the UK leaving the European Union.

3. Data

3.1 We hold a variety of data relating to individuals, including customers and employees (also referred to as "data subjects") which is known as personal data. The personal data held and processed by us is detailed within the "fair processing notice" (FPN) at Appendix 2 hereto and the data protection addendum of the terms and conditions of employment which has been provided to all employees.

3.1.1 Personal data is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by us.

3.1.2 We also hold personal data that is sensitive in nature (i.e. reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, or relates to health or sexual orientation). This is special category personal data or sensitive personal data.

4. Processing of personal data

4.1 We are permitted to process personal data on behalf of data subjects provided it is doing so on one of the following grounds:

- processing with the consent of the data subject (see clause 4.4 hereof);
- processing is necessary for the performance of a contract between us and the data subject or for entering into a contract with the data subject;
- processing is necessary for our compliance with a legal obligation;
- processing is necessary to protect the vital interests of the data subject or another person; or
- processing is necessary for the purposes of legitimate interests.

4.2 Fair processing notice

4.2.1 We have produced a fair processing notice (FPN) which we are required to provide to all customers whose personal data is held by us. That FPN must be provided to the customer from the outset of processing their personal data and they should be advised of the terms of the FPN when it is provided to them.

4.2.2 The FPN at Appendix 2 sets out the personal data processed by us and the basis for that processing. This document is provided to all our customers at the outset of processing their data.

4.3 Employees

4.3.1 Employee personal data and, where applicable, special category personal data or sensitive personal data, is held and processed by us. Details of the data held and processing of that data is contained within the employee FPN which is provided to employees at the same time as their contract of employment.

4.3.2 A copy of any employee's personal data held by us is available upon written request by that employee from Robert Ross.

4.4 Consent

Consent as a ground of processing will require to be used from time to time by us when processing personal data. It should be used by us where no other alternative ground for processing is available. In the event that we require to obtain consent to process a data subject's personal data, we shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained by us must be for a specific and defined purpose (i.e. general consent cannot be sought).

4.5 Processing of special category personal data or sensitive personal data

In the event that we process special category personal data or sensitive personal data, we must do so in accordance with one of the following grounds of processing:

- the data subject has given explicit consent to the processing of this data for a specified purpose;
- processing is necessary for carrying out obligations or exercising rights related to employment or social security;

- processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity; and
- processing is necessary for reasons of substantial public interest.

5. Data sharing

5.1 We share our data with various third parties for numerous reasons in order that day to day activities are carried out in accordance with our relevant policies and procedures. In order that we can monitor compliance by these third parties with data protection laws, we will require the third-party organisations to enter in to an agreement with us to govern the processing of data, security measures to be implemented and responsibility for breaches.

5.2 Data sharing

5.2.1 Personal data is from time to time shared amongst us and third parties who require to process personal data that we process as well. Both us and the third party will be processing that data in their individual capacities as data controllers.

5.2.2 Where we share in the processing of personal data with a third-party organisation (e.g. for processing of the employees' pension), we shall require the third-party organisation to enter in to a data sharing agreement with us in accordance with the terms of the model data sharing agreement set out in Appendix 3 to this policy.

5.3 Data processors

A data processor is a third-party entity that processes personal data on behalf of us and are frequently engaged if certain parts of our work is outsourced (e.g. payroll, maintenance and repair works).

5.3.1 A data processor must comply with data protection laws. Our data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify us if a data breach is suffered.

5.3.2 If a data processor wishes to sub-contact their processing, our prior written consent must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

5.3.3 Where we contract with a third party to process personal data held by us, it shall require the third party to enter in to a data processing agreement with us in accordance with the terms of the model data processing agreement set out in Appendix 4 to this policy.

6. Data storage and security

All personal data held by us must be stored securely, whether electronically or in paper format.

6.1 Paper storage

If personal data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. Employees should make sure that no personal data is left where unauthorised personnel can access it. When the personal data is no longer required it must be disposed of by the employee so as to ensure its destruction. If the personal data requires to be retained on a physical file then the employee should ensure that it is properly secured within the file (e.g.

stapled, or the documents are put on a Treasury Tag within the file) which is then stored in accordance with our storage provisions.

6.2 **Electronic storage**

Personal data stored electronically must also be protected from unauthorised use and access. Personal data should be password protected when being sent internally or externally to our data processors or those with whom we have entered in to a data sharing agreement. If personal data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be stored securely at all times when not being used. Personal data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

7. Breaches

7.1 A data breach can occur at any point when handling personal data and we have reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are the subject of the breach require to be reported externally in accordance with clause 7.3 hereof.

7.2 Internal reporting

We take the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the data protection officer (DPO) must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- we must seek to contain the breach by whatever means available;

- the DPO must consider whether the breach is one which requires to be reported to the Information Commissioner's Office (ICO) and data subjects affected and do so in accordance with this clause 7;
- notify third parties in accordance with the terms of any applicable data sharing agreements

7.3 Reporting to the ICO

The DPO is required to report any breaches which pose a risk to the rights and freedoms of the data subjects who are the subject of the breach to the ICO within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach.

8. Data protection officer

8.1 A DPO is an individual who has an over-arching responsibility and oversight over compliance by us with data protection laws. We have elected to appoint a DPO whose details are noted on our website and contained within the FPN at Appendix 3 hereto.

8.2 The DPO will be responsible for:

8.2.1 monitoring our compliance with data protection laws and this policy;

8.2.2 co-operating with and serving as our contact for discussions with the ICO;

8.2.3 reporting breaches or suspected breaches to the ICO and data subjects in accordance with part 7 hereof.

9. Data subject rights

9.1 Certain rights are provided to data subjects under the GDPR. Data subjects are entitled to view the personal data held about them by us, whether in written or electronic form.

9.2 Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to our processing of their data. These rights are notified to our customers in our FPN.

9.3 Subject access requests

Data subjects are permitted to view their data held by us upon making a request to do so (a subject access request). Upon receipt of a request by a data subject, we must respond to the subject access request within one month of the date of receipt of the request. We:

9.3.1 must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law;

9.3.2 where the personal data comprises data relating to other data subjects, must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the subject access request; or

9.3.3 where we do not hold the personal data sought by the data subject, must confirm that we do not hold any personal data sought by the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

9.4 The right to be forgotten

9.4.1 A data subject can exercise their right to be forgotten by submitting a request in writing to us seeking that we erase the data subject's personal data in its entirety.

9.4.2 Each request received by us will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with this clause and will respond in writing to the request.

9.5 The right to restrict or object to processing

9.5.1 A data subject may request that we restrict our processing of the data subject's personal data, or object to the processing of that data.

9.5.1.1 In the event that any direct marketing is undertaken from time to time by us, a data subject has an absolute right to object to processing of this nature by us, and if we receive a written request to cease processing for this purpose, then we must do so immediately.

9.5.2 Each request received by us will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.5 and will respond in writing to the request.

10. Privacy impact assessments

10.1 Privacy impact assessments (PIAs) are a means of assisting us in identifying and reducing the risks that our operations have on personal privacy of data subjects.

10.2 We shall:

10.2.1 Carry out a PIA before undertaking a project or processing activity which poses a high risk to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing personal data.

10.2.2 In carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that we will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data.

10.3 We will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The DPO will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the DPO within five (5) working days.

11. Archiving, retention and destruction of data

We cannot store and retain personal data indefinitely. We must ensure that personal data is only retained for the period necessary. We shall ensure that all personal data is archived and destroyed timeously and at the point that we no longer need to retain that personal data in

accordance with the periods specified within the table at Appendix 5 hereto.

Should you wish to discuss how we handle your data or what details we hold on file for you please do not hesitate to contact:

Robert Ross

Contact telephone: 0141 370 7050

Email: robert@ross-esates.co.uk