MALHOTRA & PARTNERS

PRIVACY POLICY

Contents

1. Introduction

Malhotra & Partners Letting and Managing Agents ("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, landlords, 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.

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 arti@malhotraproperties.co.uk.

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 / Point of contact 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 point of contact, rather than a DPO, whose details are noted and contained within the FPN at Appendix 3 hereto.

8.2 The DPO / Point of contact 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 / Point of contact 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 / Point of contact 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 / Point of contact 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 / Point of contact 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.

List of appendices

1. Related policies
2. Fair processing notice
3. Model data sharing agreement
4. Model data processor agreement
5. Table of duration of retention of certain data

Malhotra & Partners

GDPR Fair Processing Notice

(How we use your personal information)

This notice explains what information we collect, when we collect it and how we use this. During the course of our activities we will process personal data (which may be held on paper, electronically, or otherwise) about you and we recognise the need to treat it in an appropriate and lawful manner. The purpose of this notice is to make you aware of how we will handle your information.

Who are we?

Malhotra & Partners are a Letting and Managing Agents (Company No: 945269097) registered at 456 Cathcart Road, Glasgow, G42 7BY. We take the issue of security and data protection very seriously and strictly adhere to guidelines published in the Data Protection Act of 1998 and the General Data Protection Regulation (EU) 2016/679 which is applicable from the 25 May 2018, together with any domestic laws subsequently enacted.

We are notified as a data controller with the Information Commissioner's Office (ICO) under registration number Z1285504 and we are the data controller of any personal data that you provide to us.

Any questions relating to this notice and our privacy practices should be sent to Arti Malhotra - arti@malhotraproperties.co.uk.

How we collect information from you and what information we collect

We collect information about you:

- When you apply for housing with us, become a tenant, request services / repairs and maintenance, enter in to a tenancy agreement with ourselves howsoever arising or otherwise provide us with your personal details.

- When you apply to become a landlord.

- From your use of our online services, whether to report any tenancy related issues, make a complaint or otherwise;

- From your arrangements to make payment to us (such as bank details, payment card numbers, employment details, benefit entitlement and any other income and expenditure related information).

We collect the following information about you:

- Name;
- Address;
- Date of birth
- Telephone number;
- Email address;
- National Insurance number;
- Landlord registration number
- Immigration status and your right to reside in the U.K (if applicable);
- Income details;
- Bank account details and statements;
- Passport or driving licence numbers;
- Personal identification numbers;
- Previous addresses, dates of residency and why you left the property;
- Credit report;
- References from previous landlords;

We receive the following information from third parties:

- Benefits information, including awards of Housing Benefit/Universal Credit;
- Payments made by you to us via world pay or online banking;
- Complaints or other communications regarding behaviour or other alleged breaches of the terms of your contract with us, including information obtained from Police Scotland;
- Reports as to the conduct or condition of your tenancy, including references from previous tenancies, and complaints of anti-social behaviour.

Why we need this information about you and how it will be used

We need your information and will use your information:

- to enable us to enter a contract / tenancy agreement with you;
- to undertake and perform our obligations and duties to you in accordance with the terms of our contract / tenancy agreement with you;
- to provide the relevant local authorities and utility suppliers of your move in/out date and to advise of your forwarding/previous addresses;
- to enable us to supply you with the services and information which you have requested including our operating business hours and public holidays;
- to enable us to respond to your repair request and to forward your contact details to the relevant tradespersons / company appointed;
- to contact you in order to send you details of any changes to our services or supplies which may affect you.

Sharing of your information

The information you provide to us will be treated by us as confidential and will be processed only by our employees within the UK/European Economic Area (EEA). We may disclose your information to other third parties who act for us for the purposes set out in this notice or for purposes approved by you, including the following:

- if we enter into a joint venture with or merge with another business entity, your information may be disclosed to our new business partners or owners;
- if we instruct repair or maintenance works, your information may be disclosed to any contractor;
- if we are investigating a complaint, information may be disclosed to Police Scotland, local authority departments, Scottish Fire & Rescue Service and others involved in any complaint, whether investigating the complaint or otherwise;
- if we are updating tenancy details, your information may be disclosed to third parties (such as utility companies and local authority);
- if we are investigating payments made or otherwise, your information may be disclosed to payment processors, local authority and the Department for Work & Pensions;
- if we are conducting a survey of our products and/or service, your information may be disclosed to third parties assisting in the compilation and analysis of the survey results;
- if we are asked by HMRC in regard to taxation, your information may be accordingly disclosed;

Unless required to do so by law, we will not otherwise share, sell or distribute any of the information you provide to us without your consent.

Security

Your information will only be stored within the UK and EEA (European Economic Area).

When you give us information we take steps to make sure that your personal information is kept secure and safe. We password protect our systems and all electronic data is stored securely. All paper files are kept locked in a secure room and filing cabinets.

How long we will keep your information

We review our data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you. Our full retention schedule is available from our office, on request.

Your rights

You have the right at any time to:

- ask for a copy of the information about you held by us in our records;
- require us to correct any inaccuracies in your information;
- make a request to us to delete what personal data we hold about you; and
- object to receiving any marketing communications from us.

If you would like to exercise any of your rights above please contact us at **arti@malhotraproperties.co.uk**

Should you wish to complain about the use of your information, we would ask that you contact us to resolve this matter in the first instance. You also have the right to complain to the ICO in relation to our use of your information. The ICO's contact details are noted below:

The Information Commissioner's Office – Scotland
45 Melville Street, Edinburgh, EH3 7HL
Telephone: 0131 244 9001
email:scotland@ico.org.uk

The accuracy of your information is important to us - please help us keep our records updated by informing us of any changes to your email address and other contact details.