Data Protection Policy

Policy Statement

Everyone has rights regarding how their personal information is handled. During our business activities we will collect, store and process personal information about our staff, customers, suppliers and other third parties. We recognise the need to treat it in an appropriate and lawful manner. Any breach of this policy will be taken seriously by the company.

About this policy

The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, current, past and prospective customers and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in General Data Protection Regulations (GDPR) and other regulations. GDPR imposes restrictions on how we may use that information.
This policy has been approved by Keatons Group Limited. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

The Data Protection Officer is responsible for ensuring compliance with GDPR and with this policy. The Data Protection Officer is Claire Mardle can be emailed at headoffice@keatons.com, or written to at Keatons Head Office, 6-8 Great Eastern Street, London EC2A 3NT. Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Officer. If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with the Data Protection Officer.

Definition of data protection terms

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems. Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data. Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as an appraisal as to their actions when interacting with us). Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with GDPR. We are the data controller of all personal data used in our business. Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf. Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

Data protection principles

Anyone processing personal data must comply with the six GDPR enforceable principles of good practice. These provide that personal data must be:

(1) processed lawfully, fairly and in a transparent manner in relation to the data subject.

(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 shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.

(3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

(4) 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.

(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 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 in accordance with Article 83(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

(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.

Fair and lawful processing

GDPR is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case Keatons), who the data controller's representative is (in this case the Data Protection Officer, Claire Mardle), the purpose for which the data is to be processed, and the identities of anyone to whom the data may be disclosed or transferred.
For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required. The data subject is able to withdraw consent at any time from one or all areas where it has been given.

Electronic mail marketing

We can only carry out electronic marketing if the person we are targeting has given their permission. However, there is an exception to this rule. Known as 'soft opt-in' it applies if the following conditions are met;

(a) where we have obtained a person's details in the course of a sale/let or negotiations for a sale/let;

(b) where the messages are only marketing similar products or services; and

(c) where the person is given a simple opportunity to refuse marketing when their details are collected, and if they don't opt out at this point, are given a simple way to do so in future messages.

Processing for limited purposes

Personal data will only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by GDPR.
We collect personal data in a number of ways, for example: in branch, over the phone, via email, via online submissions, via our terms of business and using application forms. We collect information for the purpose of assisting clients and customers with their property needs and identify other services that will assist them in property related matters.
Our terms of business and documents to Sellers, Buyers, Landlords and Tenants also make clear that we collect information for administration and marketing purposes.
These documents also set out that we disclose the information to our service providers and agents for these purposes from whom we may get commission or fees.

Adequate, relevant and non-excessive processing
Personal data will only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose will not be collected in the first place.

Accurate data

Personal data will be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps will therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be destroyed.

Data retention

Personal data will not be kept longer than is necessary for the purpose. This means that data will be destroyed or erased from our systems when it is no longer required. Transaction of a sales is to be retained for seven years, after this period, data will be erased from our system, unless permission is given for us to keep in contact for marketing purposes.

Processing in line with data subjects' rights

Data will be processed in line with data subjects' rights. Data subjects have a right to:

(a) Request access to any data held about them by a data controller.

(b) Prevent the processing of their data for direct-marketing purposes.

(c) Ask to have inaccurate data amended.

(d) Prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else.

(e) Object to any decision that significantly affects them being taken solely by a computer or other automated process.

Data security

We will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

GDPR requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.
Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who are authorised to use the data can access it.

(b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes.

Personal data is therefore stored on our central computer system instead of individual PCs.

Security procedures include:

(a) Entry controls – Any stranger seen in entry-controlled areas should be reported.

(b) Secure lockable desks and cupboards – Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) Methods of disposal – Paper documents should be shredded. Online data should be deleted.

(d) Equipment - Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

Subject access requests

A formal request from a data subject for information that we hold about them must be made in writing. The initial request should be emailed to HeadOffice@keatons.com. There is then a 20 working day window in which the data needs to be provided. Any member of staff who receives a written request should forward it to the Data Protection Officer immediately.

Providing information to third parties

Any member of staff dealing with enquiries from third parties will not disclose any personal information held by us. Any enquiry made must be raised with Head Office or the Data Protection Officer, who will:

(a) Check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested;

(b) Suggest that the third party put their request in writing so the third party's identity and entitlement to the information may be verified; and

(d) Where providing information to a third party, do so in accordance with the six GDPR data protection principles.

Monitoring and review of the policy

This policy is reviewed annually by Keatons Group Limited to ensure it is achieving its stated objectives. Recommendations for any amendments are reported to the Data Protection Officer.