

---

HOUSECURE LIMITED  
DATA PROTECTION POLICY

---

## CONTENTS

Clause	Page
1. Overview .....	1
2. Management Procedures And Controls.....	1
3. The Data Protection Act Principles.....	2
4. Guiding Principles .....	3
5. Procedures For Responding To Requests For Information.....	4
6. The Sources Of Information .....	5
7. Our Use Of Your Personal Information.....	5
8. Disclosures Of Your Personal Information Within The Company .....	5
9. Disclosures Of Your Personal Information To Third Parties .....	6
10. Information Security: How We Protect Your Privacy .....	6
11. Privacy And The Internet.....	7
12. Responsibilities And Review.....	7

## 1. OVERVIEW

In the course of (i) providing our services and products to you as an individual client or as someone associated with a corporate or institutional client of the Company or (ii) as an individual employed or engaged by the Company then we expect to receive personal information about you. Obtaining, collecting and using this information is important so we can operate effectively but we also recognise that you expect us to treat this information in an appropriate manner. In addition, the Company may be under a legal obligation to collect and use certain types of information.

This Data Protection Policy describes the types of information we may collect about you, the purposes for which we use the information, the circumstances in which we may share the information and the steps that we take to safeguard the information to protect your privacy.

## 2. MANAGEMENT PROCEDURES AND CONTROLS

The Company confirms that it has adopted appropriate management procedures and implements strict controls:

- To observe fully the conditions regarding the fair collection and use of information to meet its legal obligations.
- To collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- To ensure the quality of information used.
- To ensure that the rights of people about whom information is held, can be fully exercised under the appropriate legislation which includes the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information.
- To take appropriate technical and organisational security measures to safeguard personal information.
- To provide individuals that request it with access to personal information held about them.
- To correct or erase any information on an individual that is inaccurate or misleading.
- To not use information for a purpose which is incompatible with the original purpose for which permission was given by the data subject or individual.
- To obtain clear, express permission for handling and using sensitive personal data such as race, ethnicity, political opinions, religious beliefs, trade union membership, state of health both physical and

mental, sexual life, criminal convictions and sentences and allegations of criminal behaviour.

- To treat people in a just and fair manner whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
- To allocate such resources as may be required to ensure the effective operation of this Data Protection Policy.

In addition, the Company confirms that:

- There is a designated individual with specific responsibility for Data Protection.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- There is appropriate supervision for people managing and handling personal information.
- Queries about handling personal information are to be dealt with in a prompt and courteous manner.
- Methods for handling personal information are clearly described and are evaluated at regular intervals.
- A breach of the rules and procedures identified in this Policy may lead to disciplinary action being taken against the members of staff concerned

### 3. THE DATA PROTECTION ACT PRINCIPLES

The Data Protection Act 2018 (**Act**) applies to every organisation that handles (processes) personal information. The Act has eight data protection principles which for convenience have been set out below and these are intended to guide the interpretation and implementation of the Act:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purpose(s), and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, whenever necessary, kept up-to-date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

#### 4. **GUIDING PRINCIPLES**

##### 4.1 Fair Obtaining and Processing

The Company will ensure that as far as practicable, all individuals whose details are processed by the Company are aware of the way in which that information will be obtained, held, used and disclosed. Whenever possible, individuals will be informed of the potential recipients of the information. Processing of personal information by the Company will be fair and lawful and, in addition, it is the Company's position that individuals will not be misled regarding the purposes to which the Company will process the information.

##### 4.2 Notification

The Company will not use or process personal information in any way that contravenes its notified purposes, or in any way that would constitute a breach of the Act. When appropriate, the Company will notify the Information Commissioner of any amendments to the existing Company's notified purposes or of new purposes to be added to the Notification Register entry.

##### 4.3 Information Quality and Integrity

The Company will endeavour to process personal information, which is accurate, current and of good quality. Information that is obtained by the Company will be adequate and not excessive for the purpose for which it is processed. In addition, information will be kept by the Company for no longer than is necessary for the purpose or purposes for which it was obtained.

##### 4.4 Technical and Organisational Security

The Company has implemented appropriate security measures. Information systems are installed with adequate security controls. In addition,

individuals that use these systems will be properly authorised to use them for company business.

#### 4.5 Computer Misuse

The Computer Misuse Act 1990 makes it an offence to gain unauthorised access to a computer, even if no damage is done and no files are deleted or changed. Anyone who accesses a computer without authorisation faces (i) a maximum six-month prison sentence, (ii) a maximum fine of £2,000 or (iii) both of the prior punishments.

If an individual gains unauthorised access with the intent to commit a further offence such as to purposefully change files on a computer with intent and without authorisation then the individual will potentially be subject to more severe sentences or penalties.

#### 5. PROCEDURES FOR RESPONDING TO REQUESTS FOR INFORMATION

On submission to the Data Protection Officer of a valid request for information and on receipt of payment of any appropriate costs or fees the Company shall within the prescribed time limit (i) advise the applicant as to the information that the Company holds which falls within the scope of the request and (ii) provide that information.

Please note you may be required to supply a valid form of identification as a security precaution to assist us in preventing the unauthorised disclosure of your personal information.

It should be noted that whilst individuals have a general right of access to any of their own personal information which is in our possession, the Company will be mindful of those circumstances where an exemption may apply.

In addition, the Company expects to only be required to disclose personal data to those recipients listed in the Notification Register or other entities as permitted under appropriate legislation. The Company will always endeavour to seek the permission of the data subject, where it is required by law to do so.

## **6. THE SOURCES OF INFORMATION**

The personal information we collect about you comes primarily from forms and materials you submit or provide to the Company during the course of your relationship with us. We may also collect information about your transactions and experiences with the Company relating to our products and services.

In the provision of services to you and, subject to strict compliance with all applicable legislation and regulations, information may be collected about you indirectly from other means or sources. In these circumstances, the information is not accessed on a continuous or routine basis, but it may be used for compliance or security purposes.

## **7. OUR USE OF YOUR PERSONAL INFORMATION**

The Company may use your personal information to:

- Administer, operate, facilitate and manage your relationship and/or account with the Company. This may include sharing such information internally as well as disclosing it to third parties, as described in the following two sections, respectively.
- Contact you or, if applicable, your designated representative(s) by post, telephone, electronic mail, facsimile, or alternative medium in connection with your relationship and/or account.
- Provide you with information, recommendations or advice concerning our products and services.
- Facilitate our internal business operations, including assessing and managing risk and fulfilling our legal and regulatory requirements.

If your relationship with the Company ends then we will continue to treat your personal information, to the extent we retain it, as described in this Data Protection Policy.

## **8. DISCLOSURES OF YOUR PERSONAL INFORMATION WITHIN THE COMPANY**

In order to provide efficient and reliable services and to improve product and service options available to you, more than one department or entity within the Company may be given your personal information. When sharing your personal information under these circumstances the Company will adhere to applicable legal and industry standards regarding the protection of personal information.

## **9. DISCLOSURES OF YOUR PERSONAL INFORMATION TO THIRD PARTIES**

The Company does not disclose your personal information to third parties, except as described in this Data Protection Policy. Third party disclosures may include sharing such information with non-affiliated companies that perform support services for your account or services. Non-affiliated companies that assist the Company in providing services to you are required to maintain the confidentiality of such information to the extent they receive it and to use your personal information only in the course of providing such services and only for the purposes that the Company dictates.

The Company may also disclose your personal information to fulfil your instructions, to protect our rights and interests as well as those of our business partners or pursuant to your express consent.

Please note that under limited circumstances, your personal information may be disclosed to third parties as permitted by, or to comply with, applicable laws and regulations, for instance, when responding to a subpoena or similar legal process, to protect against fraud and to otherwise cooperate with law enforcement or regulatory authorities.

Under no circumstance will your personal information be sold.

## **10. INFORMATION SECURITY: HOW WE PROTECT YOUR PRIVACY**

The Company is committed to protecting the privacy and confidentiality of your personal information. We limit access to your personal information to authorised employees or agents and, as described above in Disclosures of Your Personal Information to Third Parties, our service providers are held to stringent standards of privacy. We also maintain physical, electronic and procedural safeguards to protect the information against loss, misuse, damage or modification and unauthorised access or disclosure. Some of the other central features of our information security program are:

- The use of specialized technology such as firewalls.
- Testing of the security and operability of products and services before they are implemented as well as ongoing scanning for publicly known vulnerabilities in the technology.
- Internal and external reviews of our sites and services.
- Monitoring of our systems infrastructure to detect weaknesses and potential intrusions.
- Implementing controls to identify, authenticate and authorise access to various systems or sites.
- Protecting information during transmission through various means including, where appropriate, encryption.



- Providing personnel with relevant training and continually updating our security practices in light of new risks and developments in technology.

## 11. **PRIVACY AND THE INTERNET**

The following additional information will be of interest to you as a visitor to our site:

- Security is a co-operative effort between the Company and the users. Please remember that your details are personal to you and should not be made available to any other person. Also, you should discontinue their use and notify us if you have any reason to suspect that someone else may be using them.
- “Cookies” are small text files that may be placed on your browser when you visit our websites.
- When you visit this site, your browser may be momentarily directed to the website of an ad server or other third party service provider. This re-direction process will not be apparent to you. These third party websites automatically receive your IP address when this happens, and they may also collect information from your interaction with our websites including computer and connection information, standard web log information, and ad information. Such information does not identify you individually.
- Our websites are not currently configured to respond to “do not track” signals or similar mechanisms.

## 12. **RESPONSIBILITIES AND REVIEW**

The Data Protection Officer has overall responsibility for the administration and implementation of this Data Protection Policy with their information set out below:

[dpo@housesecure.co.uk](mailto:dpo@housesecure.co.uk)

This Data Protection Policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes, amendments or adoption of any applicable laws or regulations.