Client Privacy Statement

Here at H2 Property Services (London) Ltd we take your privacy seriously and will only use your personal information to administer your account and to provide the plumbing, gas, heating or electrical maintenance services you have requested from us.

We have no intention of sharing data with third-parties for marketing purposes.

However, from time to time we would like to contact you with important information particularly relevant to homeowners and landlords. This is by a newsletter and also may include offers and information on the services we provide.

We try and ensure that we keep our information updated and are happy to provide advice if you would like to change your subscription preferences. If in the future you decide that you wish to be removed from our mailing list it is easy to unsubscribe through the link at the bottom of this newsletter or any future newsletters we send.

Otherwise we will assume that you are happy for us to continue to hold your details and will continue to send you important news and offers.

H2 Property Services Privacy Policy

The European Union General Data Protection Regulations (GDPR) which was adopted by the European Union in 2016 will automatically come into force on 25th May 2018. The Government is introducing a UK Data Protection Bill (currently in draft) which incorporates and supplements the GDPR to create a UK data protection regime pre and post Brexit.

To comply with the law staff who process personal information must ensure they follow Data Protection Principles. The obligation to keep information confidential arises out of the common law duty of confidentiality, professional obligations and staff/third party contracts. All staff with access to confidential personal information must keep the that information safe and secure.

Purpose and Scope

This document sets out H2 Property Services' commitment to the confidentiality of personal information and its responsibilities with regard to the disclosure of such information.

It aims to ensure that all staff whether directly employed or self- employed within the company are aware of their responsibilities towards the confidentiality of personal information.

Data Protection Principles

Personal data shall be

1. Fairly and lawfully processed
2. Processed for specific purposes only
3. Adequate relevant and not excessive
4. Accurate
5. Not kept longer than necessary
6. Processed in accordance with the data subject's rights

7. Secure
8. Not transferred to countries outside the EU without adequate protection.

The Act requires H2 Property Services to register as a Data Controller with the Office of the Information Commissioner detailing the purpose for which personal information is used and use of data beyond that specified in the registration is unlawful. An annual fee is paid to the ICO's to maintain notification on the register.

H2 Property Services' registration number is: **ZA037522**

Disclosure of Personal Information

Personal information may be disclosed to engineers visiting a property in the form only of property address and contact telephone number(s), email address and names for access purposes. No other personal information is disclosed to engineers by the company.

Information Security

In order to ensure the confidentiality of personal information, systems and procedures are in place to control access to such information. Such controls are essential to ensure that only authorised persons have physical access to computer hardware and equipment and access to either electronic or paper records containing confidential information about customers.

Staff responsibilities

Staff members who process personal data about clients, staff, job applicants, or any other individual must comply with the requirements of this policy.

Staff members must ensure that:

- all personal data is kept securely;
- no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- personal data is kept in accordance with the company's Information Security Policy.
- any queries regarding data protection are promptly directed to the Data Protection Officer (Owner)
- any data protection breaches are swiftly brought to the attention of the Owner and/or Data Protection Officer
- where there is uncertainty around a Data Protection matter, advice is sought from the Data Protection Officer

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Owner and /or Data Protection Officer.

Where a third-party Data Processor is used (ie Geoop, Payment Express, Xero)

- the Data Processor must provide sufficient guarantees about its security measures to protect the processing of personal data;
- reasonable steps must be taken that such security measures are in place;

Self-employed Contractors

The company is responsible for the use made of personal data by anyone working on its behalf. Such staff must be appropriately vetted for the data they will be processing. In addition the Clinic must ensure that:

- any personal data collected or processed, in the course of work undertaken for the Clinic is kept securely and confidentially.
- all personal data processed (eg notes) is held in the company, including any copies that may have been made.
- the company receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the company.
- any personal data made available by the company, or collected, in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from the company.
- all practical and reasonable steps are taken to ensure that self- employed contractors do not have access to any personal data beyond what is essential for the work to be carried out properly.
- contractors must familiarise themselves with the principles of GDPR before they start.
- ensuring that their personal data provided to the company is accurate and up to date.

3. Subject Access Requests

The company is required to permit individuals to access their own personal data held by the company via a subject access request. Any individual wishing to exercise this right should do so in writing to the Data Protection Officer.

The company aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 14 days of receipt of the request .

4. Data Protection breaches

Where a Data Protection breach occurs, or is suspected, it should reported immediately to the Data Protection Officer.

The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved.

5. Contact

Queries regarding this policy or the Data Protection Act at large should be directed to the Owner/ Data Protection Officer.