



Data Protection & Privacy

Working for people involves holding and processing people's personal data. People have rights as to their personal information and we have responsibilities including under the General Data Protection Regulation (GDPR) which is effective from 25 May 2018.

Why this policy exists:

This policy is to help to ensure that FHF Consulting:

- Complies with data protection law and follows good practice.
- Protects the rights of clients and other parties.
- Is open about how it stores and processes people's data
- Protects itself from data breaches.

This policy helps protect FHF Consulting from data security risks including breaches of confidentiality, failing to offer choice, and reputational damage.

Data Protection Law:

The Data Protection Act 1998 describes how organisations must collect, handle and store personal information, regardless of whether it is stored electronically, on paper or in any other way. To comply with the law, this personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR provides for additional rights of people whose personal data is held. The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- the right not to be subject to automated decision-making including profiling.

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to that information.

For further information on your data rights and on people's rights under the General Data Protection Regulation, you can seek the guidance from the UK Information Commissioners Office (ICO) - <https://ico.org.uk>

The personal information we collect and use

We need enough personal information to communicate effectively with you and to enable us to do the work we are asked to do. This means sharing personal information, insofar as it is necessary.

This personal information can include:

- Name and address, phone and email details;
- ID such as driving licence and passport, NI number, bank details, welfare benefits information;
- Details of qualifications, experience, employment history;
- Information about ethnicity, gender, sexual preference, personal beliefs ;
- Medical records and reports;
- Information about criminal records;
- Information from third parties such as professional regulatory bodies

The information may be provided by you as our client, or by other people such as your GP, your bank, your regulatory body, other solicitors, schools, your employer, social services, government departments, and so on.

How we use your personal information

We use your personal information to perform our professional services in the work we have been instructed to do.

We will comply with certain principals when processing personal information:-

- We will obtain and hold personal information for specific legitimate purposes and only use it in a way that is relevant and necessary for those purposes.
- We will process personal information lawfully, fairly and in a transparent way.
- We will keep accurate and up to date personal information and take reasonable steps to delete or correct any inaccuracies without delay.
- We will not keep personal information for longer than is necessary.
- We will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

To do the work we are instructed to do generally means sharing personal data with other people or organisations. For example: barristers/counsel, experts, agents, other solicitors and advisers, the courts, witnesses, external auditors, accountants,

regulatory bodies, medical consultants and doctors, council and government departments, and so on.

Mostly, the use of your personal data will be pursuant to our contractual obligations – to do the work you want us to do - but in certain circumstances your specific consent may be needed.

We are required to store all personal data following completion of a matter for at least 7 years. Generally storage will be electronic and hard copies/papers confidentially destroyed.

Keeping your personal information secure

We take precautions to keep personal information secure so it is not accidentally lost or accessed without authority. Access to your personal information is restricted to those who have a need to know it in accordance with the purpose of the work we are doing and to meet legal requirements.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

If you have concerns

If you have any concerns please raise it with the Data Protection Manager, Keith Lomax (keith@fhfconsulting.co.uk). We would hope to resolve any query or concern. The GDPR gives the right to lodge a complaint with the Information Commissioner (<https://ICO.org.uk/concerns>) or T:03031231113.

Date: 4 May 2018