Whitworth Law - Data Protection Policy

I am required to comply with the law governing the management and storage of personal data. This is set out in the General Data Protection Regulations (GDPR). The GDPR are designed to protect individuals and the personal data, which is held and processed about them, by organisations or other individuals. The UK's Data Protection Regulator, the Information Commissioner's Office (ICO), oversees compliance with the GDPR.

This policy covers all personal data and special categories of personal data processed on my computer or stored in manual (paper based) files.

Protection of personal data and respect for individual privacy is therefore fundamental to my day-to-day operations and I have responsibility for complying with data protection by design and by default. I will always consider privacy and data protection issues at the design phase of any of business' processing activities and practices. I will ensure that I only process the data that is necessary to achieve my specific purpose.

For certain types of organisations, the GDPR requires the appointment of a Data Protection Officer (DPO). As I am a sole principal with no other staff, then I am not required to appoint a DPO but I will:

- Monitor data protection compliance;
- Fully investigate any data protection breaches;
- Ensure that I meet my obligations with regard to data protection by design and default and that Data Protection Impact Assessments are completed as and when required;
- Deal promptly with any Data Subject Access Requests;
- Liaise with the ICO and SRA, as necessary.

I will also undertake regular data protection training, at least every three years, or more frequently, if I deem it necessary.

The Data Protection Principles

GDPR is based around principles which are the starting point to ensure compliance with the Regulations. The principles require that all personal data and special categories of personal data are:

- Processed lawfully, fairly and in a transparent manner in relation to the subject;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which personal data is processed;
- Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures.

Personal Data

Personal Data means any information relating to an identified and identifiable natural person ('data subject') e.g. information from which a person can be identified, directly or indirectly. It also includes information that identifies the physical, physiological, genetic, economic, cultural or social identity of a person.

Whitworth Law - Data Protection Policy

My clients are data subjects and other individual third parties, that I hold personal data about, are also likely to be data subjects.

Special categories of data are classed as any data that reveals a person's:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade-union membership;
- The processing of genetic data or biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Processing

Data processing is any operation which is performed on personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

A data controller is the person (or organisation) that decides why and how personal data is processed. I am a data controller and I will process all personal data in a manner that is compliant with the GDPR and ensure that:

- I have legitimate grounds for collecting and using the personal data;
- I will not use the data in ways that have unjustified adverse effects on the individuals concerned;
- I will be transparent about how I intend to use the data, and draw individuals' attention to my Privacy Notice when collecting their personal data;
- I will handle people's personal data only in ways they would reasonably expect and not do anything unlawful with the data.

The conditions for processing special categories of personal data that are most relevant are:

- Explicit consent from the data subject;
- The processing is necessary to protect the vital interests of the data subject or another person;
- The processing relates to personal data that has already been made public by the data subject; or
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

I only share personal information with other individuals or organisations where it is permitted to do so in accordance with data protection law. Whenever possible, I will ensure that I have the client's (or other data subject's) consent before sharing their personal data. Although, it is accepted that this will not be possible in all circumstances, for example if the disclosure is required by law.

Lawful basis for processing data

The lawful basis for processing data is set out in article 6 of the GDPR. At least one of these must apply whenever I process personal data:

- Consent: the individual has given clear consent to process their personal data for a specific purpose;
- Contract: the processing is necessary for a contract I have with the individual, or because they have asked me to take specific steps before entering into a contract;

- Legal obligation: the processing is necessary for me to comply with the law (not including contractual obligations);
- Vital interests: the processing is necessary to protect someone's life;
- Public task: the processing is necessary for me to perform a task in the public interest or for official functions, and the task or function has a clear basis in law;
- Legitimate interests: the processing is necessary for my legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

I have recorded my processing activities and identified the lawful basis for processing the data I will hold.

Rights of Data Subjects

The GDPR gives rights to individuals in respect of the personal data that I hold about them. These rights include:

- Right of information and access to confirm details about the personal data that is being processed about them and to obtain a copy;
- Right to rectification of any inaccurate personal data;
- Right to erasure of personal data held about them (in certain circumstances);
- Right to restriction on the use of personal data held about them (in certain circumstances);
- Right to portability – to receive data processed by automated means and have it transferred to another data controller;
- Right to object to the processing of their personal data.

Data Subject Access Requests

Data subjects have the right to obtain copies of their personal data. This is known as a Subject Access Request (SAR) and I have strict time limits to comply with a SAR.

My Privacy Notice, which is available on my website, informs clients and other third parties, such as beneficiaries, of their rights as data subjects and this includes details about making a SAR. An individual can make a SAR verbally or in writing and I am alert that requests may not be clearly described as a "data subject access request".

If I receive a SAR, I will deal with it promptly and at the latest within one month of receipt. I will respond to it by letter/email having first satisfied myself that the request is from the data subject concerned, so as to avoid the risk of a serious data/confidentiality breach by sending the information to someone who is not entitled to it.

No charge will be made for responding to a SAR.

Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. They are an integral part of data protection by design and by default.

A DPIA is required for processing that is likely to result in a high risk to individuals. Therefore, if I am planning any major changes to the operation of my practice, I will undertake a DPIA. I will ensure that the DPIA considers:

- The nature, scope, context and purposes of the processing;

- Assess necessity, proportionality and compliance measures;
- Identify and assess risks to individuals; and
- Identify any additional measures to mitigate those risks.

Data Protection Breaches

I am responsible for ensuring that personal data processed is not:

- Accessed without authority;
- Processed unlawfully;
- Lost;
- Destroyed; or
- Damaged.

A data protection breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Data protection breaches can happen for a wide range of reasons, including:

- Human error;
- Cyber-attacks;
- Loss or theft of devices or equipment on which personal data is stored;
- Inadequate or inappropriate access controls;
- Deceit; and
- Disaster at my business premises.

If a data breach occurs, I will report it to the Information Commissioner's Office, no later than 72 hours, after having become aware of the breach, unless, I am satisfied that the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

I will keep a central record of any data protection breaches.

Data Retention Timescales

I have duties under legislation and other regulations to retain documents and records for certain periods of time, for example under the Limitation Act 1980 and the 2017 Money Laundering Regulations. In addition, the GDPR states that personal data should be held for no longer than necessary for the purpose for which it was processed.

I have reviewed the duties my business has in relation to the retention of data and I have set retention periods. After this time, the files will be removed reviewed and then destroyed. Any paper documents will be confidentially shredded and electronic records will be wiped.

Retention periods for personal data for clients and third parties are referred to in the Privacy Notice. The periods for which data is retained will be reviewed annually. In the event that the retention period for any class of data held is reduced, then I will take reasonable steps to review what data, within that class, is being held and take steps to remove and destroy it, as necessary.