

# Privacy Policy May 2018

This Privacy Policy has been compiled to Crawley Chiropractic Centre to comply with the General Data Protection Regulations [GDPR] 2018. The purpose of this policy is to inform the individual the means of collection of their personal data, including the security of that data; the means of processing that data; how long it is kept for; our obligations; and the rights of the Data Subject [the individual] under the GDPR.

Within our firm are two nominated individuals responsible for data under the GDPR. The roles undertaken are twofold, namely; The Data Controller and the Data Processor.

A Controller determines the purposes and means of processing personal data and a Processor is responsible for processing personal data on behalf of a controller.

As of 25<sup>th</sup> May 2018 the relevant persons within our organisation are:

Data controller: Dr Danny Scahill DC; and

Data Processor: Dr Danny Scahill DC.

To control and process data requires one of six recognised legal bases under GDPR to do so. The six bases are as follows:

1. Consent:

Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and simple ways for the withdrawal of consent will be required.

2. Contract:

Processing is necessary for a contract with an individual, or because that individual has asked that specific steps be taken before entering into a contract.

3. Legal obligation:

Processing is necessary to comply with the law (not including contractual obligations).

4. Vital interests:

Processing is necessary to protect an individual's life.

5. Public task:

Processing is necessary for the performance of a task in the public interest or for official functions, and the task or function has a clear basis in law.

6. Legitimate interests:

Processing is necessary for our 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.

# Privacy Policy May 2018

In order to rely on a 'legitimate interest' basis we undertake a three-part test which must be satisfied:

1. A legitimate interest has been identified;
2. It can be shown that processing is necessary to achieve it; and
3. Such processing has been balanced against the individual's [data subject's] interests, rights and freedoms.

Furthermore under the GDPR the Data Subject [individual] has a number of rights [seven] regarding the collection and processing of their data. For the purposes of the GDPR Data is identified under two categories:

Personal Data: Any 'personal data' relating to an identifiable person held automatically or manually.

Sensitive Personal Data: Including genetic & biometric where processed to uniquely identify an individual.

The seven rights of the Data subject are:

1. Right to be informed;

The right to be informed encompasses the obligation to provide "fair processing information". It emphasises the need for transparency in the use of personal data.

2. Right of access;

Data Subjects have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Such a Data Access Request will be provided free of charge within one month, with the following exceptions/provisos:

- a) Such a request is manifestly unfounded or excessive;
- b) Such a request is repetitive;
- c) Such a request requires copies of previously provided information.

In the event of charges being raised the firm will notify in advance such costs which in any event will be based on the administrative cost of providing the requested information.

In the event of manifestly unfair or excessive requests we may refuse to respond to the request and any such refusal will be notified to the requester [data subject] with a reason for the refusal and, in addition, information as to the data subject's rights to complain to the supervisory body or judicial authority within one month of such a request being received.

3. Right to rectification;

The GDPR gives Data Subjects the right to have personal data rectified. Personal data can be rectified if it is inaccurate or incomplete.

## Privacy Policy May 2018

4. Right to erasure;  
This right is to enables a Data Subject to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
5. Right to restrict processing;  
Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, storage of the personal data is permitted, but not to further process it. Information can be retained just enough for the individual to ensure that the restriction is respected in future.
6. Right to data portability;  
The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
7. Right to object;  
The right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics. As well as this notice to the Right to Object in this policy, we will, in all initial communications with a data subject, inform them of this right separately from any other information.

In addition a Data Subject has the right to make a complaint to the Information Commissioner's Office [ICO] on-line, by phone or in writing at the following:

<https://ico.org.uk/concerns/>

T: 0303 123 1113;

Information Commissioner's Office, Wycliffe house, Water Lane, Wilmslow, Cheshire. SK9 5AF.

The following table identifies the types of data we collect, control and process; and the legal basis we rely upon for doing so:

Type of information collected.	Purpose[s]	Legal basis for processing
Data Subject's name, address, telephone numbers, e-mail address(es).	Managing the Data Subject's relationship with the firm.	Performing the Firm's contract with the Data Subject.
Data subjects medical information	Managing the Data Subject's treatment programme with the chiropractor.	Performing the Firm's contract with the Data Subject.
Data Subject's name and email address.	Mail shot and marketing purposes.	Legitimate interest. The Data Subject may object at any time and will be informed accordingly.
Bank account details or payment details	To pay, be paid, or to refund monies.	To fulfil the contract between the Firm and the Data Subject.

## Privacy Policy May 2018

Data subject's name, address, email, next of kin.	To perform HR functions within organisation.	Contract with employee.
Data subjects name, address, bank details.	Maintain records for tax & NI purposes	Legal obligation.
Other..	Other..	Other..

How long will personal data be used for?

We will only retain personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and the Data subject's data, the purposes for which we process the data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Nevertheless by law we have to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for [six] years after they cease being customers for [tax] purposes.]

In some circumstances we may anonymise the Data Subject's data (so that it can no longer be associated with them) for research or statistical purposes in which case we may use this information indefinitely without further notice to the Data subject.

The Firm will protect the data we collect in the following ways:

The Data Subject's data will not be transferred outside the European Economic Area [EEA] without the explicit consent of the Data Subject;

The Firm has in place general recognised standards of technology including operational security including, but not limited to, data encryption thereby enabling the protection of relevant data from misuse, loss, damage, alteration, destruction or unauthorised access.

Any receipt or transfer of funds will be via recognised secure payment systems. The firm will securely destroy any financial information once used and longer needed other than required by law.

The firm's website will adhere to SSL encryption protocols.

Any breach of data which may pose a serious risk will be notified to the Data Subject without delay.

The Firm will not sell, pass on or contract with third parties Data Subject's data without prior written [withdrawable] consent other than where required to by law; or otherwise provided for in the above table; or as follows:

A Data subject's data may be passed to third parties which are under contract with the Firm to provide services to the Data Subject on the firm's behalf. In such an event the data shared is only that necessary to fulfil the service requirement under the terms of the contract with the Firm.

## Privacy Policy May 2018

Within such a contract an express condition will be that the third party keep any data secure and not to use in any other way, such data, for their own or other parties purposes.

The Firm will retain the Data Subject information for as long as necessary under the legal bases as identified in the table above or to comply with any legal obligation on the Firm's part. The firm will re view annually the data it holds to establish whether it continues to have the right to process it. Should such a right fail to continue to apply the Firm will cease from processing such data. Data may be retained thereafter in order to comply with any legal obligations which may arise.

For further information, please address any questions or comments concerning this privacy policy to Dr Danny Scahill DC, Director. Crawley Chiropractic Centre, 63 Basepoint Business & Innovation Centre, Metcalf Way, Crawley, RH11 7XX.