GDPR – Privacy Policy 2018 – HushTherapy

This document sets out the parameters within which HushTherapy acquires, controls, stores, uses and disposes of any personal data, in line with General Data Protection Regulation (GDPR) requirements.

HushTherapy is, herein after, referred to as 'We' unless specified otherwise.

What is GDPR?

"General Data Protection Regulation (GDPR) is, essentially, an upgraded version of the existing Data Protection Act legislation"

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). The GDPR sets out the principles for data management and the rights of the individual.
The General Data Protection Regulation covers all companies that deal with data of EU citizens. GDPR will come into effect across the EU on May 25, 2018. – Information Commissioner's Office

What personal data information we hold

As an organisation, HushTherapy holds a moderate level of identifiable personal data including such data as is categorised under GDPR as 'Special Category Data'.

Under GDPR, personal data is defined as *"any information relating to an identified or identifiable natural person"* Special Category data is highlighted as sensitive and therefore needs more protection. Special Category data can include details of:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

It is viewed as sensitive as, in particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

What personal data information we hold (cont.)

We hold the following client information:

- Name, Address and contact details including email address and telephone number.
- Issues which the client is presenting to us / Details of problems with which the client requires help.
- Personal history including Family details.
- Medical History and Medication Record.
- Record of progress through therapy.

We understand that client consent for treatment is not the same as GDPR consent. In the healthcare sector, client data is held under a duty of confidence. HushTherapy operates on the basis of implied consent to use client data for the purposes of direct therapy treatment, without breaching confidentiality. We obtain consent for treatment and holding of treatment related data via separate means; Our 'Consent to receive hypnotherapy treatment' form.

How we acquire this information

- Through Initial Consultation Meeting, in person or by telephone.
- Through Therapy sessions in person

Who we share this information with

In line with our ICO registration statement, we sometimes need to share the personal information we process with the individual and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons:

- family, associates and representatives of the person whose personal data we hold
- client's GP or medical/healthcare consultant etc.
- central government, police forces and security services (if applicable lawful request made)

Our lawful basis for processing personal data

We hold personal data as described above, to enable us to:

- Conduct an assessment for clients who request our help with treatment.
- Provide therapy sessions relevant to those clients.
- Track progress through therapy for our clients.
- Assess therapy 'end-point' in conjunction with our clients.

Our lawful basis for processing this data is defined under Article 9(2) of the GDPR:

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

Consent

We understand that whilst the holding of sensitive client data is lawful and held under a duty of confidence in terms of treatment, consent for us to process personal data electronically or for marketing purposes, must be:

- Freely given
- Specific
- Informed
- Unambiguous

We understand that holding client data for treatment purposes and GDPR consent are two unrelated things. GDPR consent is not a pre-condition for Therapy/treatment.

We understand the need for positive opt-in and that consent cannot be inferred from silence, pre-ticked boxes or inactivity. We will always include a quick, easy 'unsubscribe' link on our email marketing communications. We have also expressly advised our entire marketing database that they can continue to hear from us by actively 'opting-in' to clarify that they are comfortable with this.

Children

Whilst we may hold client 'Special Category' data (see page 1 for definition) for persons under the age of eighteen, which is considered as being held purely for client treatment purposes under a duty of confidence, HushTherapy will not process any of this data for any other purposes such as marketing or profiling etc. This is outlined in our 'Consent for Hypnotherapy Treatment' form.

Data Security and Retention Policy

Our IT system is backed up continuously. We have an active security policy in place to ensure that all data is backed up and held in a safe, confidential environment, including a secure, encrypted file. Our laptops have an activated encryption function in the event of theft/misuse.

We hold personal data for a minimum of 5 (five) years, and an average maximum of 8 (eight) years, in line with NHS and healthcare industry guidelines, after which time it will be deleted.

Individual's Rights

Under GDPR, we acknowledge the following rights of the individual, in respect of any personal data that we hold:

- 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

Subject Access Requests

As outlined in GDPR guidelines, we will respond to and comply with all subject access requests within one month.

If we feel that the individual's request is manifestly unfounded or excessive, we reserve the right refuse or to make a charge.

If we refuse any requests on the above grounds, we will tell the individual why and inform them that they have the right to complain to the supervisory authority and to a judicial remedy – We will do this within one month of the request.

Communication of Privacy Information

We are communicating our privacy policy via this document which will be available at all times on our website.

Registration with ICO

HushTherapy is registered with the Information Commissioner's Office. You can view our registration by visiting the Information Commissioner's Website at: www.ico.org.uk and entering the following reference number: **ZA332137**

Data Protection Officer;

Our nominated Data Protection Officer, registered with ICO is Joanne Jones – Company Director.

If you wish to discuss any aspect of this document, please contact; jo@hushtherapy.co.uk or by calling 07970 686201.

Subject access requests should be submitted in writing to: Jo Jones, HushTherapy, 'Clovelly' Nibley Lane, Nibley, Bristol, BS37 5JG