Dee Witherspoon, Complementary Therapist

Maypole Health Clinic, 3 The Barns, Maypole Road, Maldon, Essex, CM8 4SY
Mob: 07738 283858
Tel: 01621 888080

General Data Protection Regulations (GDPR)

Privacy and Data Protection Policy

GDPR brought in new legal protection for personal information from May 2018. This tells you what personal information I hold and why, and what your rights are. Once you have read it please complete and sign the Declaration of Consent at the bottom.

Policy Purpose
This policy outlines my Privacy and Data Protection Policy, and thus how I comply with the GDPR.

GDPR Registration
I have registered with the ICO (Information Commissioners Office) and this is renewed automatically each year.

Policy Content

1. The data that I process and how it passes into, through and out of my business.

Data comes into my business in 4 ways:

a. Via email messages to me from potential clients (PC) and clients (C) that have my email address.
b. Via text messages (mobile number above)
c. Via my website (www.baddowparktherapies.co.uk)
d. Via Facebook Messenger

It flows through my business via:

- My laptop - which goes from work to home
- My smart phone - everywhere I go
- My paper file - occasionally from work to home if I am working on a case study for a course

The information does not pass out of my business.

2. The Purpose of processing Client Data.

In order to give professional complementary therapy treatments, I will need to gather and retain potentially sensitive information about your health. I will only use this information for informing you about treatments and associated recommendations concerning aspects of health and wellbeing which I will offer to you.

3. What information I hold and what I do with it

- I hold personal information about my clients that they have given me. This includes name, address, contact details (telephone number(s) and email address if available), and date of birth. I also hold health and wellbeing information about them which I collect from them at their first consultation, and keep this information up to date at subsequent appointments, where appropriate.
- I hold hand written information about each treatment that they receive from me.

- I do not share this information with anyone (other than within my own practice, or as required for legal process) without explaining why it is necessary, and getting your explicit consent first.
- I use the information I have to inform my clients and provide them with any appropriate advice within the realms of the treatment as a result of my professional experience and qualifications.

4. The lawful basis for me to process personal data and special categories of data.

My requirement to hold information is for the following legal reasons:

a) Insurance purposes for which I am required to keep my records for 7 years after the last treatment
b) Law regarding children's records, for which I am required to keep my records until the child is 25, or if 17 when treated then until they are 26.
c) Registration with The Complementary and Natural Health Care Council (CNHC), for my work as a Reflexologist for which I am required to retain information for 8 years.

I also process the personal data under the Additional Condition:

- **Special Category Data - Health Related:** I process under special category data, therefore the additional condition under which I hold and use this information is for me to fulfill my role as a healthcare practitioner, bound under the FHT (Federation of Holistic Therapists), CNHC and the AoR (Association of Reflexologists) confidentiality as defined in their Codes of Practice and Ethics.

5. How Long I Retain Your Information for

I will keep your information for a period of 8 years under CNHC requirements.

Your data will not be transferred outside the EU without your consent.

6. Protecting Your Personal Data

I am committed to ensuring that your personal data is secure. In order to prevent unauthorised access or disclosure, I have put in place appropriate technical, physical and managerial procedures to safeguard and secure the information I collect from you.

I will contact you using the contact preferences you give me in relation to:

- Appointment times
- Reflexology information or information related to your health
- Special offers and promotions *(you may unsubscribe from this at any time)*

7. Your Rights

GDPR gives you the following rights:

- The right to be informed:
  To know how your information will be held and used (this notice).
- The right of access:
  To see your therapist's records of your personal information, so you know what is held about you and can verify it.
- The right to rectification:
  To tell your therapist to make changes to your personal information if it is incorrect or incomplete.
- The right to erasure (also called "the right to be forgotten"):
  For you to request your therapist to erase any information they hold about you
- The right to restrict processing of personal data:
  You have the right to request limits on how your therapist uses your personal information

- The right to data portability: *under certain circumstances you can request a copy of personal information held electronically so you can reuse it in other systems.* **Please note I do not hold treatment notes electronically, only contact information.**
- The right to object:
  To be able to tell your therapist you don't want them to use certain parts of your information, or only to use it for certain purposes.
- Rights in relation to automated decision-making and profiling.
- The right to lodge a complaint with the Information Commissioner's Office:
  To be able to complain to the ICO if you feel your details are not correct, if they are not being used in a way that you have given permission for, or if they are being stored when they don't have to be.

Full details of your rights can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/.

If you wish to exercise any of these rights, please use the contact details given above.

If you are dissatisfied with the response you can complain to the Information Commissioner's Office; their contact details are at: www.ico.org.uk

8. Therapist's Rights

Please note:

- If you don't agree to your therapist keeping records of information about you and your treatments, or if you don't allow them to use the information in the way they need to for treatments, the therapist may not be able to treat you.
- Your therapist has to keep your records of treatment for a certain period as described above, which may mean that even if you ask them to erase any details about you, they might have to keep these details until after that period has passed.
- Your therapist can move their records between their computers and IT systems, as long as your details are protected from being seen by others without your permission.

9. Processes to recognise and respond to individuals' requests to access their personal data

All individuals will need to submit a written request to access their personal data - either by email or by letter. I will provide that information without delay and at least within one calendar month of receipt. I can extend this period by a further two months for complex or numerous requests (in which case the individual will be informed and given an explanation).

I will identify the client using reasonable means, which because of the special category under which I process data. I will keep a record of any requests to access personal data.

10. Processes to ensure that the personal data I hold remains accurate and up to date.

I will ensure that client information is kept up to date during our treatments, and will update client information as I am informed of any changes.

11. Schedule to dispose of various categories of data, and its secure disposal.

Once a year I will review my client information and will place dormant clients in a separate file. This will be assessed each month to ensure that data that is no longer required to be kept under GDPR, is destroyed securely.

12. Procedures to respond to an individual's request to restrict the processing of their personal data.

As I only hold data in order to provide treatments, I cannot envisage a situation where I would receive a request to restrict their processing of an individual's personal data. However, if I do receive a request I will respond as quickly as possible, and within one calendar month, explaining clearly what I currently do with their data and that I will continue to hold their data but will ensure that it is not processed.

13. Processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability.

Should clients wish their data to be copied or transferred I would work with the client to ensure that this is done in a way that was most appropriate for them - for example this could be scanned copies of treatment received and progress made, all of which are paper based. **I do not hold any treatment information electronically.**

14. Procedures to handle an individual's objection to the processing of their personal data.

I will inform my clients of their right to object "at the point of first communication".

15. Processing operations that constitute automated decision making.

I do not have any processing operations that constitute automated decision making and therefore, do not currently require procedures in place to deal with the requirements. This right is, however, included in my privacy statement.

16. Data Protection Policy

This document also forms my Data Protection Policy and shows how I comply with GDPR. This is a live document and will be amended as and when any changes to my data processing takes place, at the very least it will be reviewed annually.

17. Effective and structured Information Risks Management

The risks associated with my data, and how that risk is managed is as follows:

- Theft of electronic devices - these have either password locks or fingerprint locks.
- Break in to office - all my paper files are stored in locked filing cabinet in a locked room.

18. Named Data Protection Officer (DPO) and Management Responsibility

Although not required to have a named DPO, I am the DPO and will ensure that I remain compliant with GDPR.

19. Security Policy

As detailed in my risk assessment. I have also chosen my electronic equipment based on their industry record as having the most robust inbuilt protection possible.

20. Data Breach Policy

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

I understand that I only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, I will notify those concerned directly and without undue delay.

In all cases I will maintain records of personal data breaches, whether or not they were notifiable to the ICO.