General Date Protection Regulation (GDPR) Policy: Nicki Holt - Issue 1 27th April 2018

Privacy and Consent Notice – Re: legislation 25th May 2018

Nicki Holt
24 Trinity Close, Fordham, Ely, Cambridgeshire CB7 5BP
07787 370755
nickiholt@guineasassociates.com

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

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

Policy Content

1. the Data that I process and how it flows into, through and out of my business.
Data comes into my business in 4 ways:

a. Via email messages to me from potential clients and clients that have my email address.
b. Via text messages 07787 370755
c. Via my website www.nickinunn.co.uk
d. Via Facebook Messenger

It flows through my business via:

- My tablet - which stays at my home address (virus scanned and protected by McAfee)
- My smart phone – always with me
- My paper file – stored in a secure cabinet at my place of work, no electronic copies are held
- My desktop computer which stays at my home address (virus scanned and protected by Eset)

The information does not flow out of my business (only in certain circumstances when requested in writing, at which point it is fully documented and recorded).

2. the personal data I hold, where it came from, who I share I with and what I do with it.
Information Asset Register

- I hold personal information about my clients that they have shared with me as a consultation questionnaire and ongoing consultation.
- This includes name, address, contact details, and, where appropriate, age. I also hold health and wellbeing information about them which I collect from them at their first consultation.
- I hold hard copy information about each treatment that they receive from me.
- I will not share your 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. It may be helpful for your treatment for me to share your information with:

a. Your General Practitioner, Healthcare professional or Complementary therapist for the following reasons:
   - For treatment planning and ongoing care planning.
   - In the interest of your health and safety

   If I am treating as the result of a referral, I have to share certain details with: The referring health professional or complementary therapist. The information to be shared would be: Proposed treatment, treatment plan recommendations and number/frequency of treatments recommended, any ongoing treatment/referrals or follow up recommendations.
   Or
b. Your Works Health Insurer
   The Information to be shared would be:
   Your contact details, treatment type, date and cost of treatment.
   For the following reasons:
   - If a receipt is requested by you.
c. Where the treatment has been provided in the case of your agreement to be a case study for my continued professional development, I will share your information with the registered trainer for that course if case studies form a requirement of my final assessment and approval to practise professionally. You name, contact details, medication and reason for medication, date of birth, occupation, presenting conditions with any medical diagnosis, your condition and relevant

markers, details of the treatment I have given you and why, comments that either of us have about the treatment/s, and changes in your condition or situation limited to the time that you are a case study.

- I use the information I have to inform my clients and provide them with any appropriate advice within the realms of the treatment, my professional experience and qualifications.
- I keep all data for:
    a. 'Claims occurring' insurance: 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. Disposal of information is conducted securely by shredding hard copy documents; a record of disposed documents is maintained.

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

I process the personal data under:

- **Legitimate interest:** I am required to retain the information about my clients in order to provide them with the best possible treatment options and advice.
- **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 fulfil my role as a healthcare practitioner, bound under the Association of Reflexologists (AoR) Confidentiality as defined in their Codes of Practice and Ethics.

4. Privacy Notice

Individuals need to know that their data is collected, why it is processed and who it is shared with. This information is included within any forms or letters I send to individuals, including at my first consultation with my client.

This privacy notice includes all of the information included in the ICO privacy notice checklist at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed#table

5. 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).
In order to confirm the identity of the client making the request I will contact them by telephone to clarify that they have made the request to receive this personal data.
I will keep a record of any requests to access personal data.

6. 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.
Once a year I will also carry out a wholesale review of all data.

7. 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.

8. 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 in writing 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.

9. 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 a hard copy of individual treatment records. I do not hold any treatment record information electronically.

10. 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 written communication" and have clearly laid this out in my privacy notice.

11. 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 this privacy statement.

12. Data Protection Policy
This document 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.
As the only member of staff I believe that I have done an appropriate amount of research around the implications of the new GDPR, including taking heed of the advice and guidance provided by my professional membership organisation the AoR.

13. 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 – all my electronic devices have password locks on, which are changed as appropriate and are not shared with anyone.
- Break into my treatment room - all my paper files are stored in a locked filing cabinet in a locked room. No one else has the key but me.
- If I temporarily remove files from my treatment room to my home I return them to the locked filing cabinet in my treatment room immediately after I have updated the information as necessary.

14. Named Data Protection Officer (DPO) and Management Responsibility
Although not required to have a named DPO, as the sole employee I am the DPO and will ensure that I remain compliant with GDPR.

15. Security Policy
As detailed in my risk assessment, I have also chosen my electronic equipment and virus protection based on advice from an IT professional.

16. 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. https://ico.org.uk/for-organisations/report-a-breach/

Data Protection Policy created: 25th May 2018
This is a live document and will be updated as and when changes occur.

Date of Next Review: 25th May 2019