Denise Owen MFHT MICHT
Massage Therapy

In-Health Chiropractic, Penybont Road, Pencoed, Bridgend, CF35 5PU
Mob: 07976 986 599 denise@deniseowen.co.uk www.deniseowen.co.uk
Five time finalist and Winner of '**BEST MASSEUSE IN WALES**' award Welsh Hair & Beauty awards, 2015

GDPR STATEMENT

By now you are all aware of the impending GDPR enforcement (General Data Protection Regulation). This affects us all, both as business owners and business users. And although GDPR may have been designed to account for new technologies, the increased threats of cyber-attacks, data breaches, and server hacks, a companies' paper documents are just as important to safeguard to ensure compliance with this legislation. And this is where GDPR affects me and my business at Denise Owen Massage Therapy.

Data Erasure

The right to erasure (the right to be forgotten) gives an individual the right to request the deletion or removal of any personal data I hold when there is ***no compelling reason for its continued processing***. This also flags up areas of compliance relating to the different forms of Data – Data in use; Data at rest and Data in transit.

For the record, all of my paper Client Consultation forms which everyone has to fill in when they come to their first appointment with me (or refresh with a new Consultation form after a long period of absence) get stored in fire-proof storage, off-site and the only person who has access to these is myself.

Under the new GDPR rules it is advisable that I appoint a Data Protection Officer (DPO) who becomes responsible for the safe storage and processing of this data. This will either be myself or my husband and if becomes my husband, he will sign a Confidentiality agreement with me to ensure no sensitive information is removed or used in any way deemed inappropriate, hurtful or irresponsible to either my clients or my business during the processing of my stored paper Consultation forms into their encrypted digital format. These final encrypted digital files will then also be stored securely off-site.

Under the new GDPR There is no absolute 'right to be forgotten'. People can ask for their personal data to be erased – but only when there is no compelling reason for its continued processing – keeping records for a minum amount of time in order to comply with business insurance would be deemed a 'compelling reason' for those records to be kept (see next section). Requests will have to be assessed on their own merits. However, care providers (and I imagine that I would come under this category), for example, will likely have a very good reason for processing much of the personal data they hold for the purposes of providing medical care.

Compelling reason for continued processing

As clients of mine, you have the right to request the complete deletion of any information that I hold about you in my data storage. But I must also make you aware that as part of my professional and my legal responsibilities under the insurance of that profession, that I have an obligation to keep and store all information held about you for a minimum of 10 years beyond the last appointment you had booked with me. This is a catch-all request, required by me to comply with, from my insurance company to ensure legal protection for both myself and my clients in case of any legal threat that might arise due to any medical symptoms experienced by my clients resulting in death or serious harm which may or may not, lawfully or unlawfully, be attributed to any treatment received by me at Denise Owen Massage Therapy. Where a client requests seeks complete removal of their data from my storage – I will seek further guidance and best practise from both my insurers and my professional governing bodies and institues as to the best course of action.

Customer consent and the 'soft opt-in' – ie Can I still text and email my clients?

Processing Personal Data – My client database and any SMS texts or emails I send to individuals regarding for example, upcoming appointments and/or new treatment availability or similar marketing contacts, would be considered ***'processing'*** – remember this word it is crucial it is the term used when we mean ***'using a customers details to contact them'***.

Do I have to gain 'consent' to communicate with my clients after GDPR?

Not necessarily. The two lawful bases for communication which I think most private companies' data processing activity will fall under are ***consent*** and ***legitimate interests***.

Legitimate Interests – at a glance

Legitimate interests is the most flexible lawful basis for processing, covering you for using people's data in ***"ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing."*** (Source: ICO https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/).

Every act of 'processing' – for example, sending an email newsletter to an existing customer – needs to stack up against three questions:

1. **Do I have a legitimate interest for sending this message? This can include your own need to cross-sell other products / services or promote wider use of an already purchased item, for example: a new therapy treatment**

2. **Do I need to send the message in order to achieve those interests? Could I reasonably achieve the same result through other, less intrusive means (such as unprompted visits to your website), legitimate interests do not apply**
3. **Have I balanced the act of sending the message against the individual's interests, rights and freedoms? This comes back to the earlier statement about reasonable expectations on their part.**

These three steps make up the Legitimate Interests Assessment (LIA).

If I (Denise Owen), choose to rely on legitimate interests, I am taking on extra responsibility for considering and protecting people's rights and interests. There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.

The processing must be necessary. If I can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply – for example if I need to tell you about a forthcoming appointment you have, I need to contact you to tell you, I cannot achieve the same result in a less intrusive way (ie. you viewing my website randomly and unprompted to see when your appointment is), I have to contact you to tell you of this information, and I rely on the ***'soft opt-in' consent*** and ***legitimate interests*** areas of the new GDPR laws to allow me to do this.

I must balance my interests against yours. If you would not reasonably expect the processing, or if it would cause unjustified harm, your interests are likely to override my legitimate interests.

My legitimate interests

My legitimate interests for contacting a client, either new or existing, would be to inform them of any forthcoming treatment appointments or to notify them that they have missed a pre-arranged treatment appointment. All client information is given to me freely by that client, either in the form of contact details over a telephone call, text, social media post or email, after they have initiated contact with me. And subsequently via the filling-out of a Client Consultation form at their first appointment, in person at my business premises. All information is voluntary on the behalf of the client, but I do stress to them that disclosure of a full medical history to me is important as certain treatments or oils used within those treatments can have adverse affects on any pre-existing medical treatments, and/or conditions.

Privacy and Electronic Communications

Whilst GDPR focusses everyone's minds on the storage of data and an individuals right to erasure of that data, we mustn't forget the other part of this whole GDPR shake-up which is the PECR (Privacy and Electronic Communications Regulations) and the new ePrivacy Regulation which will not come into affect until 2019.

Under the existing rules of the PECR if I wanted to send my clients SMS text messages or emails regarding Appointments or a Marketing opportunity ('a new therapy treatment available' for example) I cannot without specific consent – but there are exceptions to this rule when I do not need consent from my clients in order to send them my marketing emails or SMS messages.

An exemption to this rule applies here:

Emails / Texts: There is an exemption within PECR, rather ambiguously known as the "soft opt-in", whereby you can send emails/texts without Consent as long as the following conditions are met:

– You have obtained the contact details in the course of a sale (or negotiations of a sale) of a product or service
– You are only marketing your own similar products and services
– You provided a simple opportunity to refuse or opt-out of the marketing, when you first collected the contact details and in every subsequent communication.

This means you may be able to email or text your own customers without Consent, but this will not apply to prospective customers (customers I seek out and contact without their knowledge) and bought-in lists.

My resources for this information came from these references:

https://ico.org.uk/for-organisations/health/health-gdpr-faqs/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

https://www.dpnetwork.org.uk/wp-content/uploads/2017/09/DPN-Guidance-A4-Publication.pdf

https://blog.fht.org.uk/2018/02/13/gdpr-overview/

https://www.dpnetwork.org.uk/opinion/gdpr-marketers-dont-forget-pecr/

https://www.esendex.co.uk/blog/post/gdpr-and-text-messaging-what-you-need-to-know/

https://www.p4p.uk.com/gdpr-compliance-paper-documents/