Tanya Ross (Business Owner)
6 October 2022

TDR Academy GDPR Compliance Policy & Privacy Notice

Statement of policy and procedures to bring TDR Academy into compliance with the GDPR

TDR ACADEMY

OF MOVEMENT & THERAPY

MASSAGE | INJURY & PAIN MANAGEMENT

PILATES | YOGA | AERIAL FITNESS

TABLE OF CONTENTS

1. Introduction TO GDPR & TDR ACADEMY

This policy details measures taken by TDR Academy to ensure compliance with the *General Data Protection Regulation* (GDPR). The GDPR comes into force on 25 May 2018, replacing the old *Data Protection Directive* 95/46/EC. The GDPR places greater emphasis on the documentation kept by Data Controllers to demonstrate their accountability. To this end, we have performed an internal audit of our current data use and identified areas where changes are required to bring us into compliance with the GDPR.

The personal data we collect about you will include data relating to your name, address, date of birth, wider contact details and data relating to 'health' and 'injuries/illness' if applicable. We will process your personal data to allow us to provide you with our services as your health and wellness provider in quoting/charging for, arranging and administering our services to/for you, for statistical analysis and financial reporting and to assess your suitability for our services.

Your data will also be used to manage future communications between us including about our products and services. You can update your preferences or opt out from receiving such communications services at any time by clicking unsubscribe from any of the emails you receive. (Please note - we use a number of different communication software, so you may need to unsubscribe from multiple emails if you wish to be removed completely.) None of our services are automatic decision making platforms. Any information sent to you will have consent obtained either written, verbal or online.

We will only use your data for the purpose for which it was collected. We will only grant access to or share your data within TDR Academy (and Tanya D. Ross) with authorised partners, third parties and our market service providers, and for example insurance companies or medical professionals when requested by clients and where we are required or entitled to do so by law under lawful data processing.

A full copy of our Privacy Notice may be found on our website at www.tdracademy.co.uk. Our information and strategies around GDPR are implemented on advice from the Information Commissioner's Office (ICO) website (www.ico.org.uk).

2. Data currently held by TDR Academy

2.1. Information held

TDR Academy currently uses several software packages for storing data on clients, therapists & customers as well as staff and freelance teachers, including Goteampup and MindBody (studio management systems) linked with Stripe, Netbanx (online merchant bank account) and Paysafe for compliance, Mailchimp and ConvertKit (mailshot), Google G-Suite (including Microsoft Word and Excel (administrative, marketing and accounts)), YouTube, Vimeo, Pinterest, Facebook, Twitter, Instagram, LinkedIn, Whatsapp, Slack and Skype, ZOOM, TikTok, Zapier, PayPal including PayPal Here (online payment system) and Xero (accountancy package), and icloud storage. The full list is given in the Appendix (section 10). (Those marked in blue will be combined and referred to as 'social media' henceforth.) Access to all packages are password protected.

Health questionnaires and informed consent forms as hard copy documents are completed when every client attends TDR Academy for any services. On every attendance, clients are asked on their wellness and on a first visit sign asked to agree that they will update TDR Academy if there are any changes. Normal practice would be to ask the client if they have not attended for a period of 6 months to review, sign and date their written records. Any changes would be updated at that point on the online systems by that therapist or teacher. All hard copy documents are kept in locked filing cabinets with access only to those that are necessary. All information stored is private and confidential and password protected with limited accessibility to only those that require access to the information. Consent would be sought in writing from the respective client if another party required access to any information.

Safety and security are implemented through using secure sites with entrusted security platforms and using similar security systems on TDR Academy computers. Online secure payments are only taken from providers with transparent security systems and monitored compliance checks. All staff use password protected systems when accessing any information and never use open or untrusted networks. All systems used are screened as GPDR compliant in the UK. Any other systems used from outside of the UK, will be screened and monitored accordingly to ensure the safety and privacy of all data recorded.

3. Changes required for compliance with GDPR

The main finding from the audit is that our previous form for new clients, therapists and teachers (*privacy declaration and consent*) was lacking with respect to the changes required by the GDPR. We have redesigned the enrolment form to take account of these new requirements, namely:

3.1. Communicating privacy information

Our updated client form includes a declaration of who we are and how we intend to use the information provided. We add a brief section to explain:

- Who we are
- Why we need the person's information
- What we are going to do with the person's information

The privacy notice on the form directs people to our website where this GDPR policy can be found.

4. Declaring Individuals' rights

Our Privacy Statement declares:

- **individuals' rights**
    - the right to be informed
    - the right of access to their data
    - the right to rectification (changes, corrections etc.)
    - the right to erasure (removal, deletion)
    - the right to restrict processing (by third party software)
    - the right to data portability (to ask for any data held on them)
    - the right to object (to use or storage of data)
    - the right not to be subject to automated decision-making including profiling.

On the whole, these rights are the same as those under the old DPA. Our procedures are therefore already in line with these rights. Should someone wish to have their data collated, removed, changed and so on, we are able to deliver this through written contact or by clients updating their own information or unsubscribing on our online systems.

5. Gaining and managing consent

5.1. Is there a need to refresh current consent?

We did not need to refresh previous consent for the following reasons:

- In our previous registration form, new clients were asked for their medical and injury details, their contact details and those of an emergency contact to be used in a medical emergency. The contact details were also used to contact clients if there is an unscheduled change to appointments and/or class times. We currently do not require consent to retain these customer contact details because we claim this would fall under a "Legitimate interests" lawful basis for processing.

- In the old registration form, new clients were given the chance to opt in or out of their contact details additionally being used to receive any information by emails, texts, or calls. As this opt out was presented in the context of a sale (i.e. entry to an appointment or a class), we are not required to refresh consent for current clients. In addition, Recital 47 of the GDPR says that: "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

Although there is no legal obligation to refresh consent for current clients, therapists and teachers, we have nevertheless introduced new GDPR-compliant record and consent forms for all clients, therapists and teachers and this will have the effect of gradually refreshing existing consents. Parental consent will be obtained for anyone under 18, and parents will always remain present through any sessions before the age of 16 (parental presence is not required between 16-18 years of age), and the parent's details will be used for any correspondence before the age of 18. Records can be updated to reflect communication changes once the child becomes 18 and communication can be direct to them from this point forward. (Note the term parent encompasses a parent or guardian.)

5.2. Additional actions

We have contacted all teachers and therapists (all freelancers) who currently use TDR Academy to inform them of our policy and procedures, and to raise awareness of their own responsibilities under GDPR. We will do this on an iterative basis as more information becomes available, for example from some of the 3rd party systems.

We will publicly state our new systems (in brief) through a Mailchimp mailshot (including a specific link to remain subscribed in May 2018, although not required) and have this and all policies available on our website for public reference. Information on GDPR will also be included in our social media 'about' pages, if they are present, and on our website footer.

We have a subscription form to sign up for any of our email newsletters on our website and Facebook page (if used), which is GDPR compliant through both the Mailchimp, Zapier and ConvertKit interfaces.

6. 3rd-party GDPR compliance and contractual agreements

Our main client, therapist and teacher database is held by **Goteamup** (current and **MindBody** (3rd party cloud-based studio management system, in past) and data held here is periodically exported to **Mailchimp, Zapier** and **ConvertKit** (3rd party cloud-based mailshot management) and **Google** (3rd party cloud-based contacts database), and social media. GDPR requires TDR Academy to ensure these 3rd parties have their own GDPR policies and to put in place GDPR contractual agreements between TDR Academy and 3rd parties.

Mailchimp, ConvertKit, Zapier and **Google** G Suite have GDPR policies and are already in compliance with the regulations. We have GDPR contractual agreements with **Google, ConvertKit** and **Mailchimp** (adapted from templates provided by them). **Xero, Stripe** and

PayPal including **Paypal Here** have GDPR policies in place and are already GDPR-compliant, as are **Goteamup** and **MindBody**.

Any information processed directly by TDR Academy will be restricted on client request if previously opted in. If there are any direct links within any other aforementioned systems where processing is carried out, they will also be contacted as appropriate requesting the necessary update. This will be done in so far as is possible with the direct links within 1 month of the written request. If you wish to object to the processing of any stored information, the objection can be submitted verbally or in written format and the timeframe is similarly 1 month for dealing with the issue, however processing will be ceased immediately of the information requested.

7. Data retention policy

We already review our client, therapist and teacher database every two years to remove stale records (clients, therapists and teachers who have not engaged during that time). We will continue this after GDPR comes into force. Records under our professional body framework with the Federation of Holistic Therapists and insurance through Balens, are required to be kept for a minimum of 7 years from the last date of attendance and/or correspondence, with children's records from the age of 25 years (stale 7 years post 18 years of age, or after the age of 25 from the date of the last date of attendance and/or correspondence). Records may be kept for longer if justified in respect of medical information, treatment and rehabilitation from injury and/or illness or from any information regarding any insurance claims incidents. Records will be shredded securely when disposed of.

Records are portable in so far that the records are on hard copy and copies can be requested in writing. Any other personal records stored on any online system used can be requested and a file may be able to be produced of some client information allowable within the systems framework of options for emailing, or printing and collecting or posting to the client. The timeframe will be within one month for requests.

8. Procedures in the event of a Data breach

8.1. Data breach at a 3rd party data controller

The majority of our data is held by 3rd party cloud-based data controllers. Our primary CRM database is held by Goteamup and MindBody (a commercial studio management system, in past). In the event of a breach at MindBody, we would be informed by them, and the responsibility of investigating the breach would fall to MindBody and to law enforcement. In the event of a breach we would:

- inform the Information Commissioner's Office (ICO)
- inform our staff and customers as to the nature and severity of the breach
- keep our customers informed as new information was provided to us from any platform/software used that was breached
- follow the timescales advised by the ICO of reporting within 72 hours to the ICO
- record all data breaches, investigations taken and action taken.

We would follow a similar procedure in the event of a breach at our other 3rd party data controllers (Google, Mailchimp, Zapier, ConvertKit, Xero, Stripe, PayPal including PayPal Here, and all social media).

8.2. Data breach of company laptop or phone

In the event of the theft or data breach of one of our staff laptops or phones, we would:

- immediately inform the ICO
- inform our customers as to the nature and severity of the breach
- work with law enforcement to try to recover the device
- failing that, in the case of a phone, we would remote wipe it
- keep our customers informed as new information became available

9. Appointment of a Data Protection Officer

We have appointed Tanya Ross as the Data Protection Officer.

Agreed, signed and dated (on hard copy).

TANYA ROSS (business owner) 6 October 2022

Review date: 6 October 2023 or as additional information becomes available.