Claire Ferry Yoga

GDPR Compliance Policy

Statement of policy and procedures to bring Claire Ferry Yoga into compliance with the GDPR

Claire Ferry
5-23-2018

TABLE OF CONTENTS

1 INTRODUCTION

This policy details measures taken by Claire Ferry Yoga 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.

2 DATA CURRENTLY HELD BY CLAIRE FERRY YOGA

2.1 INFORMATION HELD

Claire Ferry Yoga currently uses several software packages for storing data on students & customers who provide cover, including Tula (studio management system), Mailchimp (mailshot), K-9 (local email client), Google G-Suite & Google analytics, Facebook and Xero (accountancy package). The full list is given in the Appendix (section 10).

3 CHANGES REQUIRED FOR COMPLIANCE WITH GDPR

The main finding from the audit is that our previous form for new students (*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 student 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.

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 students were asked for their contact details and those of an emergency contact to be used in a medical emergency. The contact details were also used to contact students if there is an unscheduled change to 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 students were given the chance to opt out of their contact details additionally being used to send an email newsletter. Because this opt out was presented in the context of a sale (i.e. entry to a class), we are not required to refresh consent for current students. 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 students, we have nevertheless introduced new GDPR-compliant consent forms for all students and this will have the effect of gradually refreshing existing consents.

5.2 ADDITIONAL ACTIONS

We will publicly state our new systems (in brief) through a Mailchimp mailshot (including a specific link to unsubscribe, should anyone wish) 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.

We have a subscription form to sign up for our newsletter on our website and Facebook page, which we will update to be GDPR compliant through the Mailchimp interface.

6 3RD-PARTY GDPR COMPLIANCE AND CONTRACTUAL AGREEMENTS

Our main student database is held by **Tula** (3rd party cloud-based Studio Management System) and data held here is periodically exported to **Mailchimp** (3rd party cloud-based mailshot management) and **Google** (3rd party cloud-based contacts database). GDPR requires Claire Ferry Yoga to ensure these 3rd parties have their own GDPR policies and to put in place GDPR contractual agreements between Claire Ferry Yoga and 3rd parties.

Mailchimp and **Google** G Suite have GDPR policies and are already in compliance with the regulations. We have GDPR contractual agreements with **Google** and **Mailchimp** (adapted from templates provided by them). **Xero** have GDPR policies in place and are already GDPR-compliant. We have queried **Tula** on their state of compliance and have been informed they are working on their policy. We will keep this document updated when more information is forthcoming.

7 DATA RETENTION POLICY

We already review our customer database every two years to remove stale records (customers who have not engaged during that time). We will continue this after GDPR comes into force and increase this to an annual update.

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 Tula (a commercial studio management system). In the event of a breach at Tula, we would be informed by them, and the responsibility of investigating the breach would fall to Tula and to law enforcement. In the event of a breach we would:

- inform the ICO
- inform our customers as to the nature and severity of the breach
- keep our customers informed as new information was provided to us from Tula

We would follow a similar procedure in the event of a breach at our other 3rd party data controllers (Google, Mailchimp, Xero).

8.2 DATA BREACH OF COMPANY LAPTOP OR PHONE

In the event of the theft or data breach of one of our company 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

As Claire Ferry Yoga is so closely related to Maitri Studio Ltd, and Maitri Studio is where the majority of Claire's teaching takes place, Claire Ferry Yoga will use the services of the Maitri Studio appointed Data Protection Officer, Geoffrey Moore.

Agreed, signed and dated

CLAIRE FERRY (director)

23 April 2018

Review date: 22 April 2019 or as additional information becomes available

10 APPENDIX – DATA HELD

Data held on students and customers

Data held	How gathered?	For what purpose?	How do we use it?	Held in-house and/or 3rd party?	Changes required?
Student name, email address, phone number	New student details and consent form	Contact details essential for running a studio and running an online class booking system	Online class booking system, occasionally contact students through Tula, export contacts to Mailchimp for mailshots (name and email only)	**Tula** (*3rd party cloud-based studio management system*)	Update privacy notice, consent forms
Student emergency contact details	New student details and consent form	For contacting next of kin in case of emergency involving someone at the studio	Would call next-of-kin in case of emergency at studio	**Tula** (*3rd party cloud-based studio management system*)	Update privacy notice, consent forms
Student health information	New student details and consent form	To tailor teaching according to each student's needs and pre-existing conditions	Relevant teachers can access information	**Tula**(*3rd party cloud-based studio management system*)	Update privacy notice, consent forms
Name and email	Transferred from **Tula**	For contacting people and mailshots	Seeded with imported contacts list from Tula, then automatically maintains its own copy of contacts list (auto subscribe, unsubscribe etc)	**Mailchimp** (*3rd party cloud-based mailshot system*)	No

Name and email	Transferred from **Tula**	Allows email autofill	Local copy of regularly used contacts list for android email client	**K-9** (*Android email client local to android phone*)	No
Name, email, phone number	Transferred from **Tula**	Making contacts available on mobile devices	Maintained separately from Tula CRM, for syncing contacts to android handsets	**Google contacts** for company G Suite google account (*3rd party cloud based contacts manager*)	No
Anonymized tracking token, not identifiable to any one person	N/A	Tracking analytics for company website, helps for tailoring website design and SEO strategy	Observing trends in website use over time	**Google analytics** (*3rd party cloud based anonymized tracking of company website usage*)	No
Name and whatever details shared by their Facebook account privacy settings (*held by Facebook*)	People sign up for Facebook account, then follow our Facebook page	So customers can keep up to date with news on our Facebook page	People follow us on Facebook to keep up to date	Company **Facebook** page (*3rd party cloud based social media*)	No
Student names (*only if they have paid for a class*)	Transferred from **Tula**	To track our financial accounts and allow online payment and collection	Used to track our financial accounts, produce reports and present end of year accounts	**Xero** (cloud-based accountancy package)	No
Student payment records (*only if they have paid for a class*)	Generated by day-to-day use of Tula for accounting and billing	To track our financial accounts and allow online payment and collection	Used to track our financial accounts, produce reports and present end of year accounts	**Xero** (cloud-based accountancy package)	No