Maitri Studio Limited

Maitri Studio GDPR Compliance Policy

Statement of policy and procedures to bring Maitri Studio into compliance with the GDPR

Geoffrey Moore and Claire Ferry (Company Directors)
4-23-2018

TABLE OF CONTENTS

1 INTRODUCTION

This policy details measures taken by Maitri Studio 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 MAITRI STUDIO

2.1 INFORMATION HELD

Maitri Studio currently uses several software packages for storing data on students & customers as well as staff and freelance teachers, including Tula (studio management system), Mailchimp (mailshot), K-9 (local email client), Google G-Suite & Google analytics, Facebook, Twitter, Instagram, Netgear (CCTV camera) and Xero (accountancy package). The full list is given in the Appendix (section 11).

3 CHANGES REQUIRED FOR COMPLIANCE WITH GDPR

The main finding from the audit is that our previous form for new students 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 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 and teachers, we have nevertheless introduced new GDPR-compliant consent forms for all

students and teachers and this will have the effect of gradually refreshing existing consents.

5.2 ADDITIONAL ACTIONS

We have contacted all regular teachers and therapists (freelancers) who currently use Maitri Studio 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 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 and teacher 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 Maitri Studio to ensure these 3rd parties have their own GDPR policies and to put in place GDPR contractual agreements between Maitri Studio 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 and teacher database every two years to remove stale records (customers and teachers who have not engaged during that time). We will continue this after GDPR comes into force and increase this to an annual update.

8 CCTV PROVISIONS

After a theft and attempted theft from the main hall we felt it was necessary to install a camera to monitor and record video. The aim was to deter thieves and provide video evidence in the case of a theft. There is one fixed Netgear Arlo camera that monitors the main hall and office door. The camera triggers on detecting movement and uploads the video to Netgear's servers. The videos are kept for 2 weeks and automatically deleted by Netgear. Before installation of the camera we introduced clear signage to indicate that video recording was in place. The Data Protection Officer is responsible for monitoring that the camera is functioning properly. We are registered with the ICO and have declared our use of CCTV.

9 PROCEDURES IN THE EVENT OF A DATA BREACH

9.1 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, Netgear).

9.2 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

10 APPOINTMENT OF A DATA PROTECTION OFFICER

We have appointed Geoffrey Moore as the Data Protection Officer. He is currently a co-Director and Head of IT so is well placed to have an overview of data procedures in the company.

Agreed, signed and dated

CLAIRE FERRY (director) GEOFFREY MOORE (director)

23 April 2018 23 April 2018

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

11 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
Twitter followers (*held by Twitter*)	People sign up for Twitter, then follow us	So customers can follow us on Twitter and keep up to date	People follow us on Twitter to keep up to date	Company **Twitter** account (*3rd party cloud based social media*)	No
Instagram followers (*held by Instagram*)	People sign up for Instagram, then follow us	So customers can follow us on Instagram	People follow us on Instagram to keep up to date	Company **Instagram** account (*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
Video footage of students from Netgear Arlo camera in main hall of Maitri Studio	Automatically recorded and uploaded to Netgear's servers	To deter thieves and provide video evidence in case of a theft	Footage checked only in the event of a theft or other crime taking place	**Netgear** Arlo (cloud-based video camera system)	

Data held on staff and teachers

Data held	How gathered?	For what purpose?	How do we use it?	Held in-house and/or 3rd party?	Changes required?
Teacher name, email address, phone number	Registration form when new teacher starts work	Contact details essential for running a studio and running an online class booking system	Online class booking system, occasionally contact teachers 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
Teacher 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
Teacher 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
Teacher 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 teachers 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
Twitter followers (*held by Twitter*)	People sign up for Twitter, then follow us	So customers can follow us on Twitter and keep up to date	People follow us on Twitter to keep up to date	Company **Twitter** account (*3rd party cloud based social media*)	No
Instagram followers (*held by Instagram*)	People sign up for Instagram, then follow us	So customers can follow us on Instagram	People follow us on Instagram to keep up to date	Company **Instagram** account (*3rd party cloud based social media*)	No
Teacher names, email address, phone numbers and sometimes postal address	From teachers when they join the studio or require payment	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

Teacher invoicing information (amounts invoiced, payment records etc)	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
Video footage of teachers from Netgear Arlo camera in main hall of Maitri Studio	Automatically recorded and uploaded to Netgear's servers	To deter thieves and provide video evidence in case of a theft	Footage checked only in the event of a theft or other crime taking place	**Netgear** Arlo (cloud-based video camera system)	No