This is the data protection policy of Mayoga

Introduction

Mayoga is committed to being transparent about how it collects and uses the personal data including, in particular, the data of our employees, suppliers, and actual and potential clients/customers of our services. This policy applies to the personal data of all such persons.

Data Protection Principles

Mayoga processes personal data in accordance with the following data protection principles:

Mayoga processes personal data lawfully, fairly and in a transparent manner.

Mayoga collects personal data only for specified, explicit and legitimate purposes.

Mayoga processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.

Mayoga keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

Mayoga keeps personal data only for the period necessary for processing.

Mayoga adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Mayoga tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing via this policy. It will not process personal data of individuals for other reasons. Where Mayoga relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

The Legal Basis on Which We Hold Personal Data

We hold personal data under the following permitted reasons provided by the GDPR - so one of these reasons will apply to your data:

(a) Consent: the individual has given clear consent for Mayoga to process their personal data for a specific purpose, for example: the client has input their details via Eventbrite to attend a class; emailed us to join our mailing list; signed up to our newsletter; Teaches or offers services to clients at Mayoga.

(b) Contract: the processing is necessary for a membership contract Mayoga has with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for Mayoga to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life, for example, next of kin data / emergency contact data in case of emergency.

(e) Public task: the processing is necessary for Mayoga to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for Mayoga's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, Mayoga will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;

- his/her right to complain to the Information Commissioner if he/she thinks Mayoga has failed to comply with his/her data protection rights; and
- whether or not Mayoga carries out automated decision-making and the logic involved in any such decision-making.

  Mayoga will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

  To make a subject access request, the individual should send the request to **me@mayoga.co.uk**
  In some cases, Mayoga may need to ask for proof of identification before the request can be processed. Mayoga will inform the individual if it needs to verify his/her identity and the documents it requires.

  Mayoga will normally respond to a request within a period of one month from the date it is received. In some cases, such as where Mayoga processes large amounts of the individual's data, it may respond within three months of the date the request is received. Mayoga will write to the individual within one month of receiving the original request to tell him/her if this is the case.

  If a subject access request is manifestly unfounded or excessive, Mayoga is not obliged to comply with it. Alternatively, Mayoga can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request.

  A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which Mayoga has already responded. If an individual submits a request that is unfounded or excessive, Mayoga will notify him/her that this is the case and whether or not it will respond to it.

  Other rights

  Individuals have a number of other rights in relation to their personal data. They can require Mayoga to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override Mayoga's legitimate grounds for processing data (where Mayoga relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override Mayoga's legitimate grounds for processing data.

  To ask Mayoga to take any of these steps, the individual should send the request to me@mayoga.co.uk

Data security

Mayoga takes the security of personal data seriously. Mayoga has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Data breaches

If Mayoga discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. Mayoga will record all data breaches regardless of their effect.

Individual responsibilities

Clients

Individuals are responsible for helping Mayoga keep their personal data up to date. Individuals should let Mayoga know if data provided to Mayoga changes, for example if an individual moves house or changes his/her bank details.

Teachers and Directors

Mayoga Teachers and Directors may have access to the personal data of other individuals / clients in the course of their work at the company. Where this is the case, Mayoga relies on the individual Teacher to help meet its data protection obligations for clients, as outlined below.

Mayoga Directors, Teachers and individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside Mayoga) who have appropriate authorisation;
- to keep data secure (for example by complying with these rules on to access personal data, from Mayoga's premises wit access to data, secure password protection, secure login of the MINDBODY site and app for Mayoga purposes, and not storing any client data);
- not to remove personal data, or devices containing or that can be used without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to May-Ling Foo, Founder, Mayoga, immediately. me@mayoga.co.uk

Failing to observe these requirements may lead to dismissal of the Teacher from Mayoga's schedule. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.