The GDPR and the DPA 2018 came into effect on 25th May 2018. Whilst the legislation looks daunting it is all about taking a pragmatic approach to the data you collect and making sure you use it appropriately. Collect only what you need and use it only for the purpose you have collected it for.

Please see below considerations which will help you comply with the new legislation.

1) **What information do you currently hold about your students?**

Consider:

- What personal data to you hold about your students?
- Where did this information come from?
- Who do you share it with?
- What do you do with it?
- What is your **Legal Reason** (**Lawful Basis)** for storing it?
- What did you tell them about how you would use their information?

The following are Legal Reasons (Lawful Basis) for Processing Information:

- Contractual necessity – you need to process someone's personal data to perform a contract you have with them, e.g. where you have a contract with a student to provide a product or service (yoga class).
- Legitimate interest – where you are a private sector organisation and you have a genuine and legitimate interest so long as this is not outweighed by harm to an individual's rights. This is the reason which explains why you can ask for health questionnaires to be completed, you have a legitimate interest to protect the student during a class and make necessary adjustments to meet their needs.
- Consent – your students have consented to data processing i.e. put something in your application form which allows them to tick a box to confirm that they are happy for you to store their data.
- Vital interests – it is necessary to protect someone's life.
- Legal obligation – where you need to process an individual's data because your organisation must comply with legal obligation under UK or EU law (not applicable to yoga teachers).
- Official function – you need to process data to carry out an official function or task which is in the public interest and you have a basis for proceeding under UK law. This is not relevant to teachers and applies to public bodies.

2) Decide what information you should keep

Review the privacy notices on your website or leaflets and terms and conditions – inform students why you process data, your lawful basis for processing the information, your data retention period and inform students, their information rights including that they have the right to complain to the ICO if there's a problem with the way you handle their data.

3) Check and amend your procedures

Ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format if a request is received.

4) Subject Access Requests (SAR)

You should create or update your procedures and plan how you would handle a request for information.

5) Consent

Consider how you seek, record and manage consent and whether you need to make any changes to gathering information when a new student joins a class. You have a contractual necessity to keep a student's contact details and a legitimate interest to email them information e.g. a newsletter or information about a workshop which they may be interested in. However, if you wanted to email them marketing material, particularly if they are no longer a student, then you will need to have their consent for this.

Ask students to consent to their information being stored and used for your marketing purposes when they sign up for your classes. All consent must be given freely, and if taken electronically there must be a positive opt-in, it cannot be given from inferred silence or pre-ticked boxes. This must be separate from other terms and conditions. Remember if you are emailing your students to give them the option to unsubscribe from your emails. Withdrawing consent must be as easy as giving it.

6) Data Breaches

You must ensure that you have a procedure in place to detect, report and investigate a personal data breach. This could be from hacking or simply from losing a laptop or memory stick which is not appropriately encrypted. An email sent incorrectly to the wrong person could constitute a breach, you should ensure that your email disclaimer states that if the email is sent to someone in error that it should be deleted. All organisations must notify the ICO of a breach to personal data which is likely to result in a risk to the rights and freedoms of individuals, e.g. it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, risk of embarrassment or any other significant economic or social disadvantage.

7) Appoint someone to take a lead

A member of your team (if you have one) should be appointed to take the lead for data protection compliance.

8) Employing staff

If you employ staff, ensure any of the employed yoga teachers' data is kept securely and they are aware what data you are keeping and why. You will also need to document what data you hold for them, why you are asking for it and determine a time period for keeping this information after they have left employment.

9) Former Students

Decide how long you will keep their data for. Personal data should only be kept for the time it still serves a purpose.

It is fine to keep some of their data, for example in case you need to contest a future legal issue, so with this in mind please keep your data for 7 years.

If you need to keep a sales record remove their payment details, as you have no legal reason to keep these.

Remember you will need to gather former students' consent if you plan to market to them in any way.

10) Set up a GDPR Assessment file

Store your audits, in respect of your compliance with Data Protection legislation and GDPR procedures in this file and all other information pertaining to GDPR compliance. You will need this information should the ICO ever have to investigate a complaint.

11) Children

If you teach yoga to children, then you may need to put systems in place to verify individuals' ages and obtain parental or guardian consent for any data you hold about them. The GDPR currently sets the age at which a child can give their own consent at 16.

12) Sharing Information with a Third Party

If you share your student's data with a third party, this could be a with therapist or another studio, then you will need to make your students' aware that you do this, the reasons for it and lay out what the third party will be using their information for.

For further information and expert advice contact the Information Commissioner's Office (ICO)

https://ico.org.uk/

The website has details of how to contact them, including the number of their helpline, live chat facility and advice service for small organisations.