What is GDPR?

The GDPR or The General Data Protection Regulation is new government legislation about data protection. This Regulation takes effect from 25th May 2018. As a coach you need to be aware of what it means for you. If you comply with the current Data Protection Act (DPA) this will mean you are most of the way to being compliant with the GDPR. However the GDPR does significantly increase the fines for failing to comply. Currently the highest fine under the DPA is £500,000. Under the GDPR fines for serious breaches could be up to 20 million euros or 4% of your global annual turnover.

The GDPR means that:

- You should only collect and keep the data about people that is necessary for your business and keep it for no longer than it is needed
- Data you hold on people must be kept securely
- If you seek consent from people to use their data, consent should be explicit and positively given.
- Data should only be shared with other organisations where you have consent to do so and have told people whose data you will be sharing that you will do this
- People can ask for a copy of the data you hold on them and you legally have to provide it (called a 'subject access request') and there should be no charge for this.
- People have the ability to change their data and you need to be able to amend your records.
- People have the right to be removed or to be 'forgotten' from your records.

Does this apply to me?

Almost certainly. It applies to all organisations - even if you are small, volunteer led or only have paper records. It applies to you if you collect any personal data in the course of your business – i.e. coaching or running your centre/ yard. This may include data about anyone you coach, anybody you employ and any contacts you work with. It does not include any personal data you have for solely personal or household purposes such as your personal Christmas card list.

Personal data is any information that can identify a living individual. This will include name, email, phone number, address and any other information you hold about them including any information collected before May 2018.

The Information Commissioner's Office (ICO) is the government agency that regulates data protection in the UK. Further information is available on their website which will help you to be compliant: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

What are the key changes for me?

You will need to give people **more information**. You need to tell people about how and what you do with their data when you collect it. That may be straightforward but you may be sharing it with others or storing it on an external system (e.g. stable management software). You can do this with a privacy notice or on the form you use to collect their information (i.e. an application form). You will also need to tell them the lawful basis you have for processing this personal data. You will most

likely use consent, contract or legitimate interest. Please see the ICO website for more information on this.

There will be **direct obligations** on those who process data (data processors) for you as well as on you where you collect data (data controller). This may mean if you use any third parties to process data, for example hosting your website, then you must have a written contract in place which sets out each parties' GDPR obligations.

If you rely on getting **consent** from people to use their personal data in certain ways, for example to send marketing emails, you will need to consider how you will do this in the future. Consent must now be explicit and positively given (i.e. using opt-in tick box) for each separate use of the data. A person may remove their consent at any time. Consent should be sought using simple, easy to understand terms and legal jargon avoided.

You can't keep data for longer than is necessary for the reason why it was collected. You also need to inform people how long you will keep their personal data. You can't keep it indefinitely and so you will need to decide how long you need to keep data. It must be reasonable. It is a good idea to have a policy about how long you will keep personal data (**retention policy**) and tell people about this when you collect their data.

If you are planning on putting in place a new IT system, then you need to consider whether the provider you choose has **adequate security** to protect personal data.

In some cases you may only have 72 hours to report to the Information Commissioner's Office any loss of personal data (a **breach**). Under the old Data Protection Act there were no obligations to report breaches.

There are additional protections for **children's personal data**. If you collect children's personal data then you need to make sure that your privacy policy is written in plain, simple English. And if you offer an online service to children aged 13-15, you may need to obtain consent from the parent or guardian to process the personal data.

Summary

In simple terms:

- Tell your clients what you are doing with their data.
- Get their consent to use their data for all marketing purposes and where you share their data with third parties. Be aware that people can remove their consent at any time and you should delete their details securely if they do this.
- Keep their data secure.
- Delete their data when you no longer need it.
- Be prepared to provide personal data where they request all the data you hold on them (subject access request).
- Watch out for any data breaches and report it.
- Read the guidance on the Information Commissioner's Office website:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

This document is intended for information for coaches to consider to raise awareness about GDPR. This should not be construed as advice. The sole source of recommended advice is https://ico.org.uk