Changes and Preparations

You will have already been complying with the requirements of data privacy that have been around for almost twenty years so we thought it might be helpful if we pointed out the top 10 key areas of change between the current law and GDPR.

1 - Extra Territorial Scope
The GDPR expands the territorial and material scope of the EU data protection law and applies to both controllers and processors.

2 - One Stop Shop
The GDPR introduces a one stop shop mechanism for organisations where they should be regulated by the authority for where they are based but other authorities may also be included in complaints etc.

3 - Data Processors
GDPR imposes direct obligations on data processors so that they are also subject to enforcement. Mandatory terms in processing contracts have also been expanded.

4 - Accountability
The GDPR requires you to be able to demonstrate how you comply. You therefore must keep detailed records of things such as security measures and processing details.

5 - Privacy Notices
The GDPR increases the amount of information you must provide when collecting data and that this must be done in a way that is clear and easy to understand.

6 - Consent
The GDPR introduces a higher bar for consent. It must be explicit and clear, silence or pre-ticked boxes will not be sufficient. It must also be easy for individuals to withdraw consent at any time.

7 - Individuals Rights
Individuals now have new and enhanced rights including a right not to be subject to profiling. The subject has more control over how their data can be processed. Access of each individual to their data is also to be more accessible under the GDPR.

8 - Breach Notification
You now have a mandatory obligation to notify the supervisory authority of a breach within 72 hours if you are a data controller and to notify individuals of this breach in certain circumstances. If you are a processor you only have to notify the relevant data controller.

9 - International Data Transfers
Transfers to countries outside the EEA continues to be very restricted but the GDPR does provide new mechanisms for approved certification schemes.

10 - Sanctions
The GDPR provides new wide ranging powers to the relevant supervisory authority including fines up to €20m or 4% of worldwide turnover.

Preparation for GDPR

To prepare for GDPR you should consider the attachment on 'Preparing for the General Data Protection Regulation (GDPR); 12 steps to take now' and consider how your Dojo can take steps to be compliant with the data protection principles below.

Data protection principles

The GDPR sets out a number of principles with which data controllers and processors must comply when processing personal data. These principles form the core of the obligations of each data controller and will usually form the basis of any claim that a data controller has not complied with its statutory duties.

- **Lawfulness, fairness and transparency.** Personal data must be processed lawfully, fairly and in a transparent manner. For example make sure you understand the legal basis on which you can process (*see lawfulness of processing below*) the information, make sure you are open with Dojos about how you will process their information and what you will use it for.
- **Purpose limitation.** Personal data must be collected only for specified, explicit and legitimate purposes. Make sure you clearly say why you are collecting the data what the purpose is when you are communicating with your Dojos.
- **Data minimisation.** Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Make sure you are only collecting the data that you need to contact Dojos about the CoderDojo you are running and for the benefit of your Dojo. For example, there may be good reasons to ask the age of participants or to as if they identify as female in making sure our Dojos are as good as they can be.
- **Accuracy.** Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data that you process is accurate and is then erased or rectified without delay.
- **Storage limitation.** Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed. You also need to make sure you have appropriate data security measures designed to safeguard the rights and freedoms of data subjects. Make sure that you securely delete information about Dojos who no longer come to your club or where you have not heard from the for some time.
- **Integrity and confidentiality.** Personal data must be processed in a manner that ensures its appropriate security this includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Both data controllers and data processors must use appropriate technical or organisational security measures.
- **Accountability.** If you are a data controller then you are responsible for, and must be able to demonstrate, compliance with the other data protection principles.

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights

You should check your procedures to 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.

5 Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7 Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8 Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11 Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

ico.
Information Commissioner's Office

ico.org.uk

V2.0 201705