Briefing note on the General Data Protection Regulation (GDPR)

Why is GDPR important?

It will be the new law for data protection, bringing in new requirements on data controllers and data processors. Although most of the principles and terminology have not dramatically changed the GDPR enhances rights for individuals and introduces a number of additional obligations on organisations, in particular, greater transparency and accountability.

What about Brexit?

GDPR is here to stay. It has direct effect across all European Union (EU) member states and has already been passed. Not only will the UK still be a member state on 25th May 2018 but beyond that the Government has confirmed that GDPR will form part of UK law following the country's withdrawal from the European Union. However, the GDPR does give member states limited opportunities for how it applies in their country. A Data Protection Bill is currently making its way through parliament. The Bill covers UK specific GDPR provisions and some matters outside the scope of EU law.

Terminology

Personal data – the definition has changed slightly from the Data Protection Act (DPA), for GDPR it means "any information relating to an identified, or identifiable natural person (data subject) ; and identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person".

Special categories of personal data under GDPR (formally known as Sensitive Personal Data under the DPA)

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- TU membership
- Physical or mental health or condition
- Sex life or sexual orientation
- Genetic data
- Biometric data

Note: Data relating to criminal convictions or proceedings is referred to in the draft Data Protection Bill.

February 2018

Data Subject – a living identified or identifiable individual about whom the Personal Data relates to.

Data Controller – the person or organisation that determines when, wny and how to process Personal Data. It is responsible for establishing practices and policies in line with GDPR.

Data Processor - the person or organisation which processes personal data on behalf of the Data Controller.

Process or Processing – any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Data Protection Officer – the person required to be appointed in specific circumstances under the GDPR.

The principles

The eight principles of the Data Protection Act (DPA) are:

1. Fair and lawful processing of personal data.
2. Processed for specified, lawful and compatible purposes.
3. Adequate, relevant and not excessive.
4. Accurate and up to date.
5. Not kept for longer than necessary.
6. Processed in accordance with the rights of the individual.
7. Processed with appropriate security.
8. Not transferred outside the European Economic Area without adequate protection.

The above DPA principles are contained in the GDPR as follows:

1. Lawfulness, fairness **and transparency**.
2. Purpose limitation – data collected for a specific, explicit and legitimate purposes and not further processed in an incompatible way.
3. Data minimisation – adequate, relevant and limited to what is necessary.
4. Accuracy – where necessary kept up to date.
5. Storage limitation – kept in a form which permits identification for no longer than is necessary.
7. Integrity and confidentiality – the new security principle specifies protection against unauthorised or unlawful processing and against accident loss, destruction or damage using appropriate technical or organisational measures.

There is also a new **Accountability** principle which means that a Controller is responsible for and should be able to demonstrate compliance with all of the principles. Keeping records of compliance will be important.

Transpareny is a new principle and organisations will need to provide more detailed information to a data subject when they first collect their personal data. For example how it will be used and stored as well as setting out their data subject rights (see below).

Two existing DPA principles are contained separately in the GDPR as follows:

6. The rights of data subjects - these rights are dealt with as a section of their own
8. Overseas transfer of data - transfers are covered under obligations as controllers.

FAQs

Where can I get more information?

We will continue to monitor and update these FAQ's, however the Information Commissioner's Office (ICO) has produced some guidance for small businesses and charities, including a dedicated advice line. The ICO is also updating its guidance regularly and has a number of useful toolkits. Further details are on the links below:

https://ico.org.uk/global/contact-us/advice-service-for-small-organisations

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

Do I need consent?

Consent under GDPR has been widened so it will be harder for organisations to rely on consent to process personal data.

Organisations that rely on consent to use information in certain ways, for example marketing emails will need to update the consents to meet the GDPR requirement. In particular they will need to get consent to email, post and SMS sperately and the consent will need to be as an opt-in instead of opt-out, which is currently widely used by organisations.

For other uses of information organisations will need to consider the other legal grounds for processing, for example 'legitimate interest' and communicate that to the data subject. Any grounds for processing that are established will need to be carefully considered in advance and recorded.

Do I need a Data Protection Officer?

The GDPR requires organisations to appoint a Data Protection Officer (DPO) if you:

- Are a public authority or body (other than a court);
- Carry out large scale systematic monitoring of individuals (for example, online behavior tracking); or
- Carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

The ICO will be issuing further guidance on this requirement. Once this guidance is issued organisations will be in a better place to make a decision. However, given the size and scale of clubs, Regions, and associations it is most unlikely this requirement will apply. If there is no requirement to appoint an DPO, organisations are being encouraged to have a data protection compliance lead due to the increased focus on accountability in GDPR.

What is a Personal Data Breach?

Under the DPA there are no obligations to report breaches. The GDPR contains a definition of a data breach and introduces a duty on all organisations to report certain types of data breach to the ICO (in some cases to individuals who are affected by the breach). The GDPR sets standards for security and processing which requires controllers and processors to implement appropriate technical and organisational measures.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. It may include:

- Inappropriate access controls (not using passcodes) which allow for unauthorised use
- Theft of a laptop
- Human error
- Hacking attack.

A notifiable breach has to be reported within 72 hours of the organisation becoming aware. Failure to notify of a breach could result in a fine. Organisations need to make sure that personal data is held securely and devices are password protected.

What are the enhanced data subjects' rights and how will they affect us?

Subject access request are not new, however, under GDPR they must be complied with in one month. Although this can be extended where requests are complex or numerous. Also, under GDPR the £10 fee has been removed, however ICO guidance states you can charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive. Such requests usually arise where there is a dispute. Make sure you keep a log of how and when you respond. ICO guidance is available on their website.

The right to erasure ('right to be forgotten') enables individuals the right to request that personal data be deleted and removed where there is no compelling reason for its continued processing.

What are the fines?

The penalties for non-compliance are stricter. Currently the highest fine the ICO can impose is a maximum of £500,000. Under GDPR this will rise to:

- Maximum fine of up to 10 million euros or 2% of annual turnover (whichever is greater) for less serious breaches such as not maintaining written records or a failure to conduct a privacy impact assessment where required).
- Maximum fine of up to 20 million euros or 4% of annual turnover (whichever is greater) for serious breaches (such as a breach of the basic principles for processing or infringement of data subject rights).

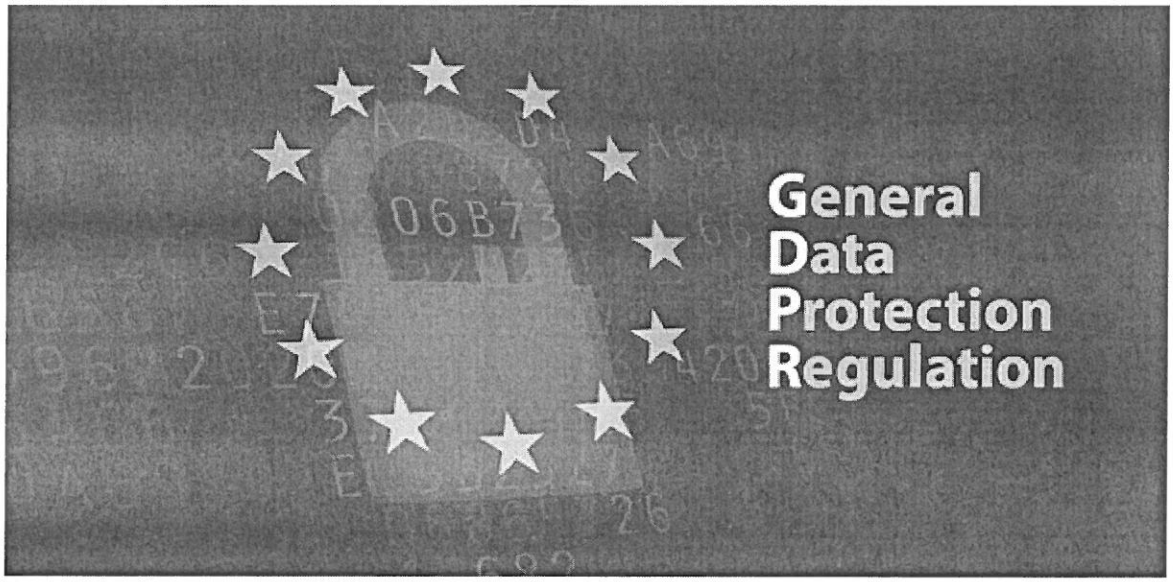
Such fines are designed to punish and not just deter. Although the ICO has recently indicated it will take a proportionate approach to fines and has highlighted other sanctions (such as warnings) available to it.

Do I need to register as a data controller?

Under the DPA some organisations were required to register with the ICO as data controllers. Under GDPR registration will no longer be required but organisations that were registered as data controllers will still have to pay a fee. The fee structure and process has yet to be finalised and some exemptions such as those available to not-for-profit organisations are likely to continue to apply.

Swim England

Follow us:



Important information about new GDPR legislation

Dear Secretary,

As you will probably be aware, from **25 May 2018** the new law for data protection, GDPR, wil be coming into effect.

GDPR brings in new requirements on data controllers and data processors. Although most of the principles and terminology have not dramatically changed the GDPR enhances rights for individuals and introduces a number of additional obligations on organisations, in particular, greater transparency and accountability.

We have produced a separate summary of GDPR that you can **read here**.

What steps to take now?

The Information Commissioner's Office (ICO) has created a number of useful resources around some of the general aspects of GDPR. However, of the key areas of guidance are stil under consultation. The ICO has produced some guidance for small organisations, including a dedicated advice line. The ICO helpline number for small organisations is 0303 123 1113, then select option four. Further information is available via the links below.

- **Practical advice for small organisations**
- **12 steps to take to prepare for GDPR**

Of the 12 steps to take, the following will be particularly relevant to clubs, counties and regions:

Awareness

Make sure your committee, volunteers and staff are aware of data protection issues and that the law is changing.

Information you hold

Document what personal data you hold, where it came from and who you share it with. Depending on what systems you already have in place you may need to undertake a mini-audit to map data flows. This will also act as a reference document for any compliance

efforts. Swim England will explain to members how data given through the online membership system will be used but clubs for example will need to document information stored on their own event/club management software and explain to their members how it wil be used. To assist with this process we will be providing a data audit template that will be made available on the website during the course of next week.

Identify lawful basis for processing data
The lawful basis for processing needs to be identified and documented. They are broadly the same as in the current Data Protection Act (DPA) and in most scenarios clubs, counties and Regions will seek to rely on legitimate interest grounds for lawful processing. For example to administer training sessions or administer an individual in an event they have entered or may wish to enter.

Consent
Review how you ask for and record consent. Under GDPR organisations are likely to rely on other lawful bases for processing rather than rely on consent, which has been widened by GDPR. However, you will still need consent to send marketing emails to your members. Consent for marketing will need to be clear, with individuals positively opting in, using unticked boxes with sufficient information in order that a clear yes can be indicated in relation to what is being sent to them.

Subject access requests
Under GDPR organisations will only have one month (currently 40 days under the DPA) to deal with subject access requests. Documenting where you hold information will assist in handling requests within the new timescales.

This guidance and briefing note are a general summary of GDPR. This and the further guidance we will be providing is aimed at assisting clubs, counties and regions to address the additional requirements under GDPR. Where organisations have specific concerns that are not addressed by general guidance then specialist advice may need to be sought.

Swim England
Pavilion 3, SportPark, 3 Oakwood Drive
Loughborough University, Leicestershire, LE11 3QF