Member briefing: What you need to know about General Data Protection Regulation (GDPR)

September 2017

Introduction

This briefing aims to help you understand the basics of the General Data Protection Regulation (GDPR) and how it will impact your organisation. We also hope that it will help you to consider what changes may be required.

GDPR imposes new rules around data protection for any organisation that collects and uses data about EU residents. The new regulation will have an impact on all sport and recreation organisations and it will change the way that we handle, use and store data about the people we engage with. The regulation is designed to strengthen existing data protection laws for all individuals who reside in the EU.

The new rules will come into force in the UK from 25th May 2018. The Government has confirmed that the UK's decision to leave the EU will not affect the commencement of GDPR.

We have identified 10 questions that will help you to get to grips with GDPR. These are:

Why has the EU changed the rules around data protection?

The EU has reformed its laws around data protection for a variety of reasons. One of the main reasons cited is to help generate business in the EU by simplifying rules for companies in the Digital Single Market. More than 90% of Europeans said they want the same data protection rights across the EU[1]. The GDPR aims to achieve this by having one set of EU-wide rules that will do away with fragmentation and the costly administrative burdens of complying with different pieces of national legislation, leading to savings for companies who operate in Europe of around €2.3 billion a year[2].

Another key reason is to strengthen citizens' fundamental data rights in the digital age. Two thirds of Europeans, according to a recent Eurobarometer survey, stated that they are concerned about not having complete control over the information they provide online. Furthermore, seven out of ten Europeans worry about the potential use that companies make of the information they have disclosed[3]. The GDPR reforms will strengthen an individual's right to data protection and aim to give them more trust when they hand over their personal data.

What is 'personal data'?

Personal data is defined as any piece of personal information that can be used to identify an individual, either directly or indirectly[4][5]. This includes information such as an individual's:

- Name
- Telephone Number
- Email address
- Date of birth
- Health information
- Location data
- Online identifier e.g. IP addresses or cookies

What is 'sensitive data'?

The GDPR defines 'sensitive personal data' as data which reveals an individual's:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade Union membership;
- Genetic or biometric details, where processed to uniquely identify an individual;
- Health details.

Under the GDPR regulations, organisations are banned from processing sensitive data, unless the individual gives the data holder his or her permission or processing is allowed in specific cases[6].

---

[1] http://europa.eu/rapid/press-release_IP-15-6321_en.htm
[2] http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_en.htm
[3] http://europa.eu/rapid/press-release_IP-15-6321_en.htm
[4] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
[5] http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_en.htm
[6] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

What are the six privacy principles?

To comply with GDPR, organisations will have to meet six privacy principles[7]. These are:

1. Personal data must be processed lawfully, fairly and in a transparent manner;
2. Personal data must only be collected for "specified, explicit and legitimate purposes";
3. Data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Personal data must be accurate and where necessary kept up to date;
5. Personal data that is no longer required should be deleted;
6. Processors should ensure all personal data they hold is secure.

What are the lawful bases an organisation can process data?

Under the GDPR, an organisation can lawfully process data only if at least one of the following conditions are met[8]:

- The data subject has given their consent;
- If the processing is necessary for the performance of a contract;
- For compliance with a legal obligation;
- If the processing is necessary to protect the vital interests of the data subject;
- Public interest purposes;
- If there is a legitimate interest pursued by the data holder or a third party.

What rights does an individual have?

The GDPR reforms create some new rights for individuals when their personal data is being processed, as well as strengthen some of the rights that currently exist under the Data Protection Act[9]. These rights are:

The right to be informed:

An individual has the right to be informed whenever their personal data is being processed. Any information an organisation supplies about the processing of an individual's personal data must be:

- Concise, transparent, intelligible and easily accessible;
- Written in a clear and plain language, particularly if addressed to a child;
- Free of charge.

The information an organisation must supply to an individual is determined by whether or not the organisation obtained that individual's personal data directly from them[10]. More information on this can be found in the briefing produced by the Information Commissioners Office (ICO).

The right to access:

[7] http://www.consultancy.uk/news/13487/six-privacy-principles-for-general-data-protection-regulation-compliance
[8] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/
[9] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/
[10] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-be-informed/

Under the GDPR reforms, an individual will have the right to obtain access to their personal data and confirmation that their data is being processed. This is similar to existing rights to access data that exist under the Data Protection Act.

Any information requested by an individual must be provided without delay and at the latest within one month of receipt. The information must also be provided free of charge, although the organisation who holds the data can charge a 'reasonable fee' if a request is repetitive or excessive. The data holder could also refuse to respond if they feel the request is manifestly unfounded or excessive, provided they explain why they have chosen to do so to the individual who made the request and inform them of their right to complain[11].

The right to rectification:

An individual has the right to ask for any wrong or incomplete information an organisation holds about them to be rectified. Any third parties who have had access to the personal data in question must also be informed about any changes. Any request for rectification must be answered within one month[12].

The right to erasure:

Also known as the 'right to be forgotten', this right allows an individual to request the deletion or removal of personal data that is held about them. However, this right can only be applied by an individual for a specific set of reasons, including:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally intended;
- When the individual withdraws their consent;
- When the individual objects to an organisation processing their data and there is no overriding legitimate interest to continue the processing;
- If the organisation holding the data is in breach of GDPR;
- The personal data must be erased in order to comply with a legal obligation;
- The personal data is processed in relation to the offer of online services to a child (which requires parental permission).

A data holder can refuse a request from an individual to erase their data for the following reasons:

- If it compromises freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For public health purposes;
- For research purposes that are in the public, scientific or historical interest;
- The exercise or defence of legal claims.

If the erased personal data has been shared with third parties, the data holder must inform those third parties that the data needs to be erased[13].

---

[11] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-of-access/

[12] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-rectification/

[13] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-erasure/

The right to restrict processing:

An individual has the right to ask the data holder to restrict the processing of their data if they have legitimate grounds to do so, though the data holder can still store the personal data.

The data holder is required to restrict the processing of an individual's data on the following grounds:

- If an individual contests the accuracy of their data;
- If an individual has objected to the processing, and the data holder is considering whether its legitimate interests over ride those of the individual;
- When processing is unlawful and the individual requests restriction instead of erasure of their data;
- If the data holder no longer needs to store the personal data but the individual requires the data for a legal claim.

If a data holder has had to restrict the processing of personal data, it must inform any third parties with whom they have shared that data of the processing restriction[14].

The right to data portability:

An individual has the right to obtain and reuse their personal data for their own purposes across different services. This new right allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure manner.

An individual's right to move their data only applies to:

- Personal data that an individual has provided to a controller;
- Where the processing is based on the individual's consent or for the performance of a contract;
- When processing is carried out by automated means.

This data must be provided in a structured, commonly used and a machine-readable format, so that other organisations can use the data. The personal data must also be provided free of charge and must be handed over within one month[15].

The right to object:

An individual has the right to object to the processing (in particular for scientific/historical research purposes) or direct marketing of their personal data, although an individual can only raise an objection based on "grounds relating to his or her particular situation".

The data holder must stop processing the personal data unless:

- They can demonstrate legitimate reasons for the continuation of processing the personal data which over-rides the interests, rights and freedoms of the individual; or
- The processing is related to legal claims.

[14] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-restrict-processing/

[15] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-data-portability/

The data holder must also inform individuals of their right to object "at the first point of communication" and in a privacy notice[16].

Rights relating to automated decision making and profiling:

An individual has the right not to be subject to an automated decision intended to evaluate certain personal aspects relating to them, such as their performance at work, reliability, conduct etc. An automated decision is one in which technology is used to automatically make decisions, e.g. profiling someone to predict their performance or health. Fully automated decisions are rare, as most decisions do still have an element of human intervention. But they are becoming more commonplace, hence why this has been included.

This right applies if:

- The decision is based on automated processing; or
- The decision has a legal or similar effect.

However, this right does not apply if the decision:

- Is necessary for entering into a performance of a contract between the data processor and the individual;
- Is authorised by law;
- Based on explicit consent.

Where necessary, the data holder must ensure that an individual is able to:

- Obtain human intervention;
- Express their point of view;
- Obtain an explanation of the decision and challenge it[17].

What are a sport and recreation organisation's obligations as a data holder?

The 'accountancy principle' requires you as data holders to demonstrate that you comply with the principles. To be able to demonstrate that you comply, you must:

- Create and implement appropriate internal data protection policies such as staff training, internal audits of processing activities and reviews of internal HR policies;
- Record data processing activities;
    - If you have less than 250 employees you are only required to record high-risk data processing e.g. data that is related to criminal convictions/offences;
- Check if you need to appoint a Data Protection Officer (The ICO has more information on whether you will need one);
- Run impact assessments to anticipate any issues around data protection, particularly for high risk processing;
- Protect any personal data that you hold using appropriate security e.g. data about participants, volunteers, staff etc;
- Protect the rights of people who give you their data (see above) by ensuring your organisation has the right systems in place to be able to observe those rights;
- Ensure the data you are processing is secure and is kept confidential;

[16] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-object/

[17] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/rights-related-to-automated-decision-making-and-profiling/

- Ensure that data is only collected in your organisation for specified, explicit and legitimate purposes and is kept accurate and up to date;
- Review how you get consent to use personal data and ensure the criteria for making data processing legitimate is observed;
- Build data protection safeguards into services from the earliest stages of development;
- The GDPR only applies in countries that are part of the EU. Members should therefore ensure that, if personal data is being transferred to countries that sit outside of the EU/EEA, that these countries guarantee an adequate level of protection to their data[18][19].

These obligations are also relevant to individual local sport and recreation clubs, not just national governing bodies. So you will need to share these requirements with your clubs and work with them to ensure they are compliant with the new regulations.

What happens when there is a data breach?

Under the GDPR, organisations holding data will be required to report certain types of data breach to the Data Protection Authority and, in some cases, to the individuals affected by the data breach.

The GDPR defines a personal data breach as a "breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".

The Data Protection Authority, which for the UK is the ICO, must be notified of any data breach that will result in a risk to the rights and freedoms of individuals e.g. it will result in discrimination, damage to reputation, loss of confidentiality etc. If this risk is particularly high, then the individuals who are affected must be notified.

Any data breach must be reported to the ICO within 72 hours of the organisation being made aware of it. Failure to notify a breach when required to do so can result in a fine of up to €10 million Euros or 2% of your turnover[20].

What happens if I break the rules?

The ICO will be monitoring whether organisations are complying with the GDPR regulations. Any failure to do so will result in the ICO issuing anything from a warning to a fine of up to €20 million Euros or 4% of your annual turnover[21].

What are the benefits for members of these changes?

Whilst the new GDPR rules will require members to devote significant resources to thinking through and – where necessary – changing how you store and use your data, they will also result in a number of benefits to your organisation, such as:

- The new regulation will strengthen your data protection policies, thus minimising the risk of any misuse of data or data fraud occurring in your organisation;
- Rethinking the way you store and process personal data gives you the opportunity to use your data more efficiently and productively;

---

[18] http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_en.htm
[19] http://ec.europa.eu/justice/data-protection/files/eujls08b-1002_-_protection_of_personnal_data_a4_en.pdf
[20] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/
[21] Ibid

- Removing data you don't need will result in less wasteful data management and processing;
- If you need to process data abroad in a country that is in the EU, then having to deal with a single pan-European law for data protection will save you time and money;
- If an individual chooses to take advantage of the new right to data portability when joining a sport or recreational activity, then it will make it easier for you and your clubs to obtain and re use their details;
- The increased levels of security that compliance with GDPR requires will protect you more widely from cyber-attacks;
- The new regulation will give you the opportunity to increase your reputation for being trustworthy to do business with.

Further reading

If you would like any further information on anything to do with GDPR, there a number of sources that can provide this.

- The ICO have produced a detailed briefing on GDPR and what organisations should do to prepare for the new regulations;
- The European Commission has produced a number of factsheets on the GDPR regulations;
- Microsoft have produced a range of resources to help organisations comply with GDPR;
- Our corporate partner Microtrading are helping the Alliance and a number of other organisations in the sport and recreation sector to become compliant with GDPR;
- As mentioned in the introduction, we will be producing further resources on GDPR in partnership with our corporate partners as well as running a members' learning event later this year, so look out for future updates on this.