

## 2.3 GDPR Advice



[SportCheer NI]

As a community sports club, you will already be familiar with the Data Protection Act [1998] which requires any organisations that manage personal data to adhere to data protection legislation.

However, in May 2018 the management of data will see significant changes, particularly regarding accountability and how data is captured following the introduction of the General Data Protection Regulation [GDPR]. The GDPR is the culmination of several years' work across the EU community reflecting the dynamism of technological changes and, about these changes, how data is managed and stored. In the UK presently the DPA outlines organisations' obligations, provides guidance and issues fines where appropriate under the auspices of the Information Commissioner's Office [ICO].

It is important to note that the GDPR will not only supersede the DPA, but also on how organisations manage and control personal data is increased.

However, please bear in mind that if you are already complying with the requirements of the DPA, your clubs approach to data management will provide a sound foundation to the GDPR changes. This means that you can apply what you are already doing as good practice while taking into account that you will be required to make adjustments and implement new procedures to comply with GDPR for sports organisations. What follows is a breakdown of the principles of the GDPR and how sports organisations are impacted, with advice on the best approach for your group to take.

### GDPR Principles

#### Collection and Use of Data

If your sports club collects and uses personal data, the GDPR will apply directly to you and place legal requirements on how you manage and store data.

This mainly applies to sports clubs who use databases that store information including names and contact details of its members, fans and others.

#### Membership

Under GDPR you will be expected to give people a clear explanation on why you are collecting their data. In other words, you must provide clarity on what you will use their information for i.e if it is as a record of their membership/attendance at your sports club, you will need to tell people this and, moreover, you will be expected to say to them if you intend to share their information with any third parties. Third parties could include sponsors who might wish to use data for marketing purposes, as well as governing bodies and local authorities. The bottom line for you to remember is that you are required to tell people whose data you are collecting, why you need it and what you will use it for.

By being explicit, this gives people the option of accepting or declining the use of their data.

#### Who Is Accountable?

Under GDPR, accountability extends to anyone who collects, manages and stores information on the people who use your sports club.

This is applicable not only to the data controller, who is the person responsible for the overall management of data but also to data processors. A data processor might be a staff member or volunteer in your club, or it could be an external party, such as a website host or data storage platform who you pay to manage your club's data collection and storage. It is worth mentioning that under GDPR if you do use third parties in this regard, it is very

likely they will have legal protections embedded in the agreement so that if any data breaches occur, it could mean that the data controller in your organisation carries overall accountability. If your club relies on volunteers, it is imperative that they fully understand their responsibilities if they are involved in data management.

Again, the salient point to remember is that your data controller carries the responsibility for your data management, which incorporates all of your data processors whether they are paid or voluntary.

## Consent

If you are applying the DPA guidelines currently, you will already be obtaining consent from individuals to collect, manage and store their personal information.

Under GDPR, you are required to be explicit in why you want their data and what you intend to do with it. The GDPR has a laser focus on the rights of the individual whose information is being collected, which includes the right to be informed and the right to restrict processing. What this latter point means for your club is that you will be obliged to tell people how you intend to use their data, mainly if you want to share it with third parties, and the individual has the option to either give or refuse their consent.

The GDPR places the onus on organisations who use personal data to be crystal clear on how they use it, and therefore approval might prove more problematic in some instances.

However, as long as you explain to people why you are collecting their data, you will not be in breach of the GDPR regulations, regardless of whether consent is given or refused.

## Privacy And Data Management Declaration

Your sports club will most likely have a standard statement on the data collection forms you currently use, but under GDPR you must ensure that any statements are wholly explicit in why you have personal data, what you intend to do with it as well as providing adherence to the individual's right to privacy. If you think your statement needs adjustment to factor in these elements, then act as soon as possible to effect these changes.

## Children

GDPR applies extra protections for management of children's details, and this will apply to any sports club where children are members/attend. Out with parental or guardian consent, if you are collecting data directly from children, under the new GDPR regulations you will need to ensure your data capture statement is produced in terms that children will understand and without overly complicated terms.

## Transfer of Data

You will only be able to use personal data for its primary purpose unless you obtain the permission of the person to transfer their details to another party.

So, for example, if your sports club collects personal information for membership purposes, that is the primary purpose.

Any sharing of a person's details must only be done with the express knowledge and therefore permission of the person, otherwise, under GDPR this will be treated as a data breach.

## Data Access

Keep in mind that any data you hold on individuals will be accessible by them under what is known as a subject access request. Under the DPA regulations, organisations can charge a fee of £10, but the GDPR changes will allow requests free of charge. However, on rare occasions where repeated requests are submitted, you can obtain guidance from the ICO on how to proceed, as requests must be reasonable and proportionate. Multiple requests

from the same individual, for example, could be viewed as contentious. Therefore, with the removal of the £10 fee, consult with the ICO if this becomes an issue for your club.

When Do I Need To Start Making Changes?

GDPR-TODO-LIST-web You need to review your data policies and procedures as soon as possible.

## 12 STEP GUIDE

What Will Happen If There Is A Data Breach?

Under GDPR rules, you must inform the ICO of any data breach within a strict timescale of 72 hours.

The ICO will review the circumstances and consequences of the breach, and levy fines where appropriate.

The fines will be heavier than they are now under the DPA but will remain proportionate to the nature of the breach and the size of the organisation.

Anyone who manages data will need to be able to recognise when a breach has taken place, and who they need to inform at your sports club.

It is the data controller's responsibility to contact the ICO, whereas under the present DPA there is no obligation to alert the regulator.

Is There Any GDPR Training Available?

Make sure that anyone in your club who manages data is up to date with legislation and the forthcoming changes, and you must include volunteers where applicable.

You can access checklists for both data controllers and data processors on the ICO's website as a starting point.

These will give you a picture of what you will need to implement or adjust, as well as identifying any areas you need to give particular focus to.

The ICO also has a range of GDPR training videos and webinars, and resources such as e-learning, stickers and posters to maintain proper data management together with practical advice for data controllers.

To begin, look at the ICO GDPR guidance document and then go through the checklists

## FREE CHECKLISTS

What Documents Do I Need To Use For GDPR?

There are useful templates available including the following:

Example Data Protection Statement

Sample Data Protection Policy

Full Explanation of Data Protection Principles

#### SAMPLE CLUB MEMBERSHIP FORM

#### Conclusion

Although some of these changes might seem daunting, it could be useful to spend some time considering how personal data is managed throughout your club.

Taking a GDPR overview of your processes can help you focus on what might need improvement, what is working well and areas that could require specific attention under GDPR.

gdpr-save-the-date-webIf you manage personal data, ask yourself what kind of information you collect and do you need it.

Think about what you tell individuals when you are gathering their data, how and where you are storing it, and when are you deleting data.

Similarly, review IT systems where appropriate, and make sure ICT is secure, with file encryption and password protection on all computerised documents and programmes that store data.

As long as you give yourself sufficient time for planning and preparation, including the training of appropriate staff and volunteers, your sports club can continue to manage personal data securely.

Reputation and trustworthiness are essential elements of any organisation, and with the increasing challenges of a changing technological world, GDPR regulations serve to underpin the importance of data management as an integral part of good business practice.