General Data Protection Regulation (GDPR)

Issue date: 13th May 2018

General Data Protection Regulation (GDPR)

Contents

Introduction 2
- Definitions 2
- Personal data 2
- Special categories of personal data (Sensitive personal data) 2
- Processing 3
- Data controller 3
- In Practice 3
- Notification / registration 3
- Data audit 3
- Accountability and governance 4

The Practicalities 6
- Membership Information 6
- Former members 6
- Member listings 6
- Entries for club events 7
- Giving Data to others 8
- Expelling / disciplining members 8
- Looking after data / security 8
- CCTV 9

The Law 10
- Types of data 10
- Collecting and keeping data 10
- Using data 11
- Storing data 12
- Access to data you hold/Subject Access Request 12
- Individuals' Rights 12
- Children 13
- Data Breaches 13
- Penalties 13

SAA Responsibility Statement 14

Introduction

Data Protection law in the UK will undergo some significant changes with the introduction of the General Data Protection Regulation (commonly referred to as the **GDPR**). The GDPR will replace the current Data Protection Act from 25 May 2018. (The Government has confirmed that "Brexit" will not affect the GDPR from coming into effect so you cannot ignore it.) The changes require some forward planning and may require changes in your forms and procedures.

This guidance note gives an overview of how the GDPR is likely to apply to SAA clubs. The uses you make (and want to make) of the information about living individuals which you obtain will be governed by the GDPR and we recommend that you adopt now the policies and procedures you will need under the GDPR.

It is a good opportunity to assess what information you really need, make sure it is up to date and that you obtain it in accordance with the GDPR. Failure to comply with the GDPR will attract very much higher penalties than now.

Definitions

The GDPR relates to **personal data** and **special categories of personal data**.

Personal data

Any information relating to an identified or identifiable natural person (referred to as the **Data Subject**). A person is identifiable if they "*can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors, specifically the physical, physiological, genetic, mental, economic, cultural or social identity of that actual person*".

Special categories of personal data (Sensitive personal data)

Personal data "*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*".

The special categories of personal data do not include personal data relating to criminal convictions and offences but there are similar extra safeguards in relation to those types of data.

Processing

"A*ny operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, determination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

Data controller

"The natural or legal person, public authority, agency or other body which, alone or jointly, with others determines the purposes and means of the processing of personal data".

In Practice

Most, if not all, the information you request on your membership application forms, event entry forms and which you collect from visitors, suppliers, staff and volunteers will be personal data. That will include names, addresses, dates of birth, telephone numbers, and e-mail addresses. However, personal data can also include opinions held about someone and can include references to them in emails or other communication. Information about health and physical disabilities will be sensitive personal data to which additional safeguards apply.

Given the extent of the definition of "processing", you should assume that any use you make, or want to make, of the personal data, as well as your collection, storage and destruction of it, will be governed by the GDPR.

Notification / registration

The requirements for organisations to "register" with the ICO is being removed by the GDPR and replaced by the general accountability obligation to demonstrate compliance with the data protection principles.

Data audit

The GDPR is a more extensive piece of legislation than the existing Data Protection Act. However, if you are already complying with the Data Protection Act you are likely to be well on the way to compliance with the GDPR.

You should establish whether your current policies and procedures are suitable to comply with the GDPR. If not, you should alter them.

Start with a review to assess:

- what personal data you hold;
- whether you need it;
- where it came from and the basis on which it was collected;
- what you do with it and are planning to do with it;
- where and how you store it.

You will need to document this.

You may have obtained the consent of the individual to whom the data relates when you originally collected it. If so, you should have told them, at the time you collected the data, what you would use it for.

If you cannot clearly identify that you have consent (in accordance with the GDPR) then you should consider whether you can use the data on one of the other bases of processing (see section **Collecting and keeping data**). If not, then you will have to collect the data again, with the appropriate consent request. The most convenient time to do this is on renewal of the individual's membership but if that is after 25 May 2018 you need to be aware that you risk not being compliant with the GDPR when it comes into force. It is very important that the data is only used for the purposes which were made clear to the individual at the time the data was collected. You cannot, therefore, collect data for the purposes of managing a member's membership and then use it to, for example, send them marketing information. If your records are unclear or if you have held the information for a long time you may need to collect fresh data with appropriate consents so that you know that it is "clean".

Accountability and governance

The GDPR makes the principles of accountability and transparency far more significant than under the Data Protection Act. You must be able to demonstrate that you comply with the data protection rules.

There are specific obligations on maintaining records which apply particularly to organisations with 250 employees or smaller organisations where the processing is not occasional or includes sensitive persona data or is likely to result in a risk for the rights and freedoms of the data subject. Whilst the obligation to maintain records is unlikely to apply to the majority of SAA clubs we advise.

A prudent approach is to have a data protection policy which records:

- the purposes of the processing;
    - the categories of data subject and the categories of personal data which relate to them;
- the recipients / categories of recipients of the personal data;
- any overseas transfers of the personal data;

    - general indication of time limits for erasure of the different categories of personal data;
- description of technical and organisational security mechanisms you use.

You should identify this information in any event in order to decide what steps you need to take to comply with the GDPR.

Whilst it will not be mandatory for clubs to appoint a Data Protection Officer it would be prudent for someone at the club to take ownership of the role. Getting ready for the GDPR is likely to take some time and will require considered thought to develop suitable processes and policies and, thereafter, ongoing management. Appointing someone or a team of volunteers within your organisation to take ownership of the process is likely to be necessary.

Data protection rules are enforced by the Information Commissioner. The Information Commissioner's Office (ICO) has a website (ICO.org.uk) which contains very useful information. This Guidance Note contains links to some of that guidance which is likely to be particularly relevant.

The Practicalities

Membership Information

Only collect the information which you need and be clear on the application form (whether paper or online) what you will use the information for. (See section **Collecting and keeping data**). Store application forms securely.

Consider:

- who needs to see them;
- how long they need to be kept;
- the relevance of the application form once the applicant has been accepted or rejected.

If your application form asks the applicant to provide bank details (e.g. for direct debit purposes) separate the financial information from the rest of the application.

- Store financial information separately from the application form. If the application is rejected, destroy the financial information – you no longer need it.
- If your application form is online and you take payment electronically use a recognised online secure payment system.

Make sure that you keep all membership information up to date. Ask members to check their information at renewal and provide an easy method for them to provide you with up to date information.

Former members

Store separately the information you hold about former members from the information you hold about current members (whether on paper or electronically). Securely destroy all financial information you have about them.

- Consider the purposes for which you need to retain information about former members and record the reasons and the time period. (See **Storing data**).
- Destroy all information about former members in line with your Retention Policy.

Member listings

Consider the purposes of your member listings. They must only contain the information necessary to fulfil those purposes (e.g. the usual purpose of a member listing is to enable members to contact each other so name of member and telephone number is likely to be sufficient). It is unlikely that there is a need to include members' home addresses in the listing.

You can only include a member's details in your member listings if they agree that you can do so. Your application form must contain a box for them to tick (or something similar) to show they have agreed. You cannot use a pre-ticked opt-in box nor an opt-out box.

The form must therefore make clear the information to be included in the member listing. They must be able to change their mind at any time and no longer be included in the Member listing.

- If your Member listing is online then updates should be made regularly.
- If your Member listing is in hard copy then you should update it and circulate it annually. In that case you should make clear, when you seek consent for a member's details to be included, that their details will be included for the whole year.

You cannot make membership of the club conditional on a member agreeing to have their name in the Member listing.

Entries for club events

Only collect the information which you need and be clear on the application form (whether paper or online) what you will use the information for. Store application forms securely. Consider:

- who needs to see them;
- how long they need to be kept;
- the relevance of the application form once the applicant has been accepted or rejected or the event completed.

If your application form asks the applicant to provide bank details for payment purposes, separate the financial information from the rest of the application.

Store financial information separately from the application form. If the application is rejected, destroy the financial information – you no longer need it

If your application form is online and you take payment electronically use a recognised online secure payment system.

If a sponsor or other third party of the event wants the details of those taking part you can only provide that data to the sponsor or third party if the individual entrants agree. The application form for the event needs to make clear that you wish to pass their data to the sponsor or third party and must give them a box to tick if they agree.

- Consent requires a positive opt-in under the GDPR (you cannot use pre-ticked opt-in boxes or opt out boxes).
- Entrants must be able to change their mind at any time and you must provide an easy way for them to do so.
- You cannot make entry to the event conditional on a participant agreeing to allow their name to be made available to the sponsor or third party.

Giving Data to others

The basic rule is that you cannot pass any data you have about individuals to anyone else (e.g. sponsors or third parties of events, other clubs) without the agreement of the individual (See sections **Entries for club events**, and **Expelling / disciplining members** for further information).

If you are being asked to provide data about a member to anyone other than that member, you should seek legal advice.

If another organisation (e.g. an insurance company) wants you to send out information about their services to your members, you are not able to do that unless you have the agreement of each person to whom you are going to send the information.

Expelling / disciplining members

If you decide to discipline a member:

- Opinions about a member are personal data and so the member could require to see that data through a subject access request.
- The member is entitled to make a subject access request and ask for the data you hold about their discipline / expulsion and any other personal data you hold about them.
- Data about the member's expulsion are data relating to that member so other members do not have the right to see that data.
- If others object to a member's discipline you cannot disclose the data to them – they must obtain it from the member (if the member is willing to provide it to them).

There are issues of confidentiality as well as data protection. See Section **Access to data you hold / Subject Access Request**

Looking after data / security

You have a responsibility to look after data which you hold. You must take particular care of financial information as there is a serious risk to the owners of that information if it falls into the wrong hands.

Your security obligations must be taken equally seriously whether you hold data in hard copy or electronically. See section **Storing data** for a link to advice from the Information Commissioner.

Data in hard copy form should be kept in a locked cabinet to which access is restricted. It is preferable for appropriate steps to be taken to provide secure storage at your club premises if that is practical and is likely to be safe. If that is not practical or if you don't have club premises and you have hard copy data then it must still be kept securely. Therefore if the data is kept at an officer's home it should still be in a locked cabinet to which access is restricted.

If you store data electronically be very careful if it is stored in "the Cloud".

Cloud computing means access to computing resources on demand i.e. access to hardware and/or software.

Cloud computing carries data protection risks which are not always obvious. Generally you, as the cloud customer, will be the data controller and have overall responsibility for complying with data protection rules. Cloud computing is not a “one size fits all” and so the data protection issues which apply can vary. If you are using cloud computing you should ensure that you have a written agreement with the cloud services provider. You may need to seek legal advice on the agreement and the data protection provisions which it should contain.

It is important you know in which country the cloud service provider stores your data. If it is outside the EU/EEA you have additional responsibilities.

There is guidance from the ICO about cloud computing at https://ico.org.uk/media/1540/cloud_computing_guidance_for_or ganisations.pdf

Whether data is stored in hard copy or electronically you should consider who should be able to access which data e.g. the Treasurer may be the only officer who needs access to financial information. If so, the financial information should be stored in such a way that only the Treasurer can get access to it plus perhaps one other person in the event of an emergency if the Treasurer is ill or away.

Data held electronically should be encrypted.

If you have arrangements with suppliers who process personal data on your behalf (e.g. the printer of your members' directory) the GDPR requires you to have a written agreement with them containing certain provisions.

CCTV

The images of individuals obtained through CCTV are personal data and therefore subject to the GDPR.

The general principle is that you must be clear about the purposes for which you are using CCTV and can then only use the images for that purpose (e.g. crime prevention).

There is extensive guidance from the ICO on the use of CCTV at https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

The Law

Types of data

You are likely to collect all or some of the following data:

- Name, address, date of birth, e-mail address, phone numbers and other contact details of members.
- Names of joint members or children who live at same address as a member.
- Types of membership.
- Date of joining the branch.
- Renewal information and fees.
- Name, address, e-mail address, phone numbers and other contact details of suppliers, staff, volunteers, coaches and instructors.
- Name, address, date of birth, e-mail address, phone numbers and other contact details of participants in events such as try dives or other branch run events.
- Event lists (which includes names and possibly other details of members).
- Medical information of members

Collecting and keeping data

Data can only be processed lawfully, fairly and transparently. You can only process (and therefore collect) personal data in certain circumstances:

- Consent of the Data Subject
- The legitimate interests of the data controller.
    - Necessary for the performance of the contract with the data subject.
- Compliance with a legal obligation to which you are subject.
    - Necessary to protect the vital interests of the data subject or of another natural person.
    - Necessary for performance of a task carried out in the public interest.

We recommend that, as far as possible, you only collect data which is necessary for the performance of the membership contract with the member. You can rely on that basis where, for example, you use information on an application form in a way which is necessary for the purposes of the membership of the applicant. So you can use contact details to notify members of, for example, branch events and training requirements, without needing consent each time, but you are not able to include a member's details in a club directory without their consent. You should not assume that you can rely on your "legitimate interests" as data controller for all processing. Although that reason may be available to you it should not be regarded as a "catch all" and it is highly unlikely that it will be a valid basis for compiling a membership directory which is made available to members.

- You must record the basis on which you collect and use data.
- You must only collect the data you need for the purposes you have specified.

When you collect data you must provide the data subject with certain information:

- Your identity and contact details.
- How you intend to use their data.
- Your lawful basis for processing their data.
- Details of anyone who may receive the data.
- Your data retention policy.
- The individual's right to complain to the ICO if they believe there is a problem with your handling of their data.

You must make sure the data remains accurate so therefore you must keep it up to date.

You must keep the data for no longer than is necessary for the purpose for which you obtained it. If you make sure that you dispose of data when you no longer need it you reduce the risk that it will become inaccurate, out of date or irrelevant and therefore reduce your security risk.

Using data

You may only use personal and sensitive personal data you have collected for the purposes you specified at the time you collected it. If you are relying on Consent as the basis for your use of the data, you need to be aware that the GDPR requirement for consent is more stringent than under the Data Protection Act:

- Consent must be given freely, be specific, be informed and be unambiguous.
- There must be a positive opt-in - you cannot infer consent either from inactivity, silence or pre-ticked boxes.
- Consent must be separated out from any other terms and conditions.

Individuals must be given the right to withdraw their consent at any time and this must be as easy to do as it was to give consent in the first place.

The ICO has a 2 page checklist of things to consider and include when you are seeking consent at https://ico.org.uk/media/for-organisations/documents/1625126/privacy-notice-checklist.pdf.

Whilst you may have relied on obtaining the data subject's consent for information which you already hold you need to check that the consent you have complies with the GDPR requirements.

You must keep evidence of the consent.

Storing data

You should have a data retention policy that takes into account the purposes for which the data is kept, for how long the data needs to be kept (and why) and how the data will be destroyed. You should not be tempted to keep all data indefinitely "just in case".

General correspondence between your organisation and a member may only need to be kept for a short period. Correspondence relating to a potential claim or disciplinary matter may need to be kept for a number of years.

Personal and sensitive personal data must be kept securely. You should consider the risks and decide on your levels of security accordingly. You must take appropriate measures to prevent unauthorised or unlawful processing of the data and against accidental loss or destruction of, or damage to, the data.

There is useful guidance on IT Security from the ICO at https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

Personal data cannot be transferred to a country or territory outside the EEA unless that country or territory provides a suitable level of protection for data.

Access to data you hold/Subject Access Request

An individual can ask to see the data you hold about them. This is known as making a Subject Access Request.

- The GDPR allows one month from the receipt of the request to respond.
- The GDPR does not allow you to charge a fee for responding to a Subject Access Request unless it is manifestly unfounded, excessive or repetitive.

The ICO has useful guidance on subject access requests at https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/

Individuals' Rights

Under the GDPR individuals have various rights, such as:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- The right not to be subject to automated decision-making including profiling.

Children

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity. For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. In short, if your organisation collects information about children – in the UK this will probably be defined as anyone under 13 – then you will need a parent or guardian's consent in order to process their personal data lawfully. Remember that consent has to be verifiable and that when collecting children's data, your privacy notice must be written in language that children will understand.

Data Breaches

You must have documented procedures to detect, report and investigate data breaches.

A data breach is a breach of security which leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A breach is therefore more than just losing personal data.

If the breach is likely to result in a risk to the rights and freedoms of anyone, you have to notify the ICO. This has to be considered on a case by case basis. You need to consider the potential detrimental effect on the individual (for example discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage).

If a breach is likely to result in high risk to the rights and freedoms of anyone then you have to notify the individuals concerned.

Penalties

Under the GDPR the penalties for breach are significantly greater than under the DPA.

The following are links to cases where the ICO has imposed fines on organisations for failing to follow data protection rules. These have been imposed under the Data protection Act 1998 but show the breaches in which the ICO may take action.

https://ico.org.uk/action-weve-taken/enforcement/data-breach-by-historical-society/

https://ico.org.uk/action-weve-taken/enforcement/bloomsbury-patient-network/

https://ico.org.uk/action-weve-taken/enforcement/data-breach-by-barrister/

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/06/warning-to-smes-as-firm-hit-by-cyber-attack-fined-60-000/

If you have any queries, questions or comments on the information contained in this document, please contact Irene Sartorius at dpo@saa.org.uk.

SAA Responsibility Statement

The information contained in this guidance represents the SAA's interpretation of the law as at the date of this edition. The SAA takes all reasonable care to ensure that the information contained in this guidance is accurate and that any opinions, interpretations and guidance expressed have been carefully considered in the context in which they are expressed. However, before taking any action based on the contents of this guidance, readers are advised to confirm the up to date position and to take appropriate professional advice specific to their individual circumstances.