Insight

GDPR

General Data Protection Regulation (GDPR)

Guidance for MSA-registered clubs

CHAPTER 1: PREPARING FOR GDPR

As a club, it is important that you comply with data protection laws. New legislation known as the General Data Protection Regulation (GDPR) will replace the existing Data Protection Act from 25 May.

This document provides guidance to MSA-registered clubs in the run-up to the GDPR effective date. It assumes that you are already compliant with the existing Data Protection Act, but don't worry if you are not sure because we will be providing plenty of information and links to other resources to help you through the journey.

The purpose of this first chapter is simply to introduce you to GDPR and help you to understand how and why it affects your club.

What is GDPR?

GDPR is new EU-wide **data protection legislation**, which the Information Commissioner, Elizabeth Denham, says is about "greater transparency, enhanced rights for citizens and increased accountability." **Transparency** is key to handling data fairly and lawfully.

In more detail, GDPR aims to **bolster data protection** in all areas by providing: coherent rules, simplified procedures, coordinated actions, user involvement, more effective information and stronger enforcement powers. Under GDPR, those who handle personal data have **greater responsibility** to protect that data effectively, through appropriate, pragmatic and proportionate security measures. What's right for our largest clubs may not be necessary for our smallest clubs.

Who does GDPR apply to?

GDPR applies to **all organisations** operating within the EU. Since **your club** processes personal data, it **must follow GDPR**. Our clubs vary tremendously in size and activity, and the size of an organisation will be a factor in a range of areas, including the requirement to maintain data processing records.

However, **even small organisations are not exempt** from GDPR, so whether yours is a small club with 25 members or a larger club with 1000 members, it will still need to follow the Regulation.

How is GDPR enforced?

Enforcement by supervisory authorities is central to GDPR. In the UK, the supervisory authority is the **Information Commissioner's Office (ICO)**. If there is a breach of the GDPR, the ICO will consider how the breach happened (for example intentionally or accidentally), what procedures the club has, the number of people affected, whether those people are damaged by the breach, and what – if any – action was taken to mitigate the damage.

However, most data breaches at club level would be unlikely to get anywhere near the ICO. If you do have an accidental breach, the important thing is for the club to learn from the error and update its processes to stop it from happening again.

There has been a lot of talk about **fines** under GDPR, however the Information Commissioner has said that "it's **scaremongering** to suggest that we'll be making early examples of organisations for minor infringements

or that maximum fines will become the norm." If your club understands the requirements, has procedures in place and stays alert then you have no need to worry about fines.

Should our club register with the Information Commissioner's Office (ICO)?

In answering this question, the first point to make is that whether your club does or does not register with the ICO, it is still bound by the law and must therefore follow with GDPR.

The ICO has an online self-assessment facility to help you **determine whether you should register**. Please **CLICK HERE**. Many of our smaller clubs may not need to register.

What are the key things we need to do NOW to prepare for GDPR?

To help you prepare for 25 May, you should take some time to consider the following questions and fill in any gaps that you uncover:

- **What personal data** does your club hold about people?
  - Start by making lists of all types of information you hold: member details, vehicle information, entry information, programmes, results and volunteer details are just a few
- **What** do you use the data for and **who** controls it or uses it?
  - Try to draw up a data map showing where data is and how it flows in and our of your club
- **How** secure is the personal data that you hold and **where** is it?
  - Start to write a procedure for how the information is handled so that you can show your security measures are appropriate for the size of your club. Think about access to PCs, laptops, tablets, USB sticks, phones and how to protect those devices, such as with passwords or even encryption
- Do you take steps to keep personal data **up-to-date** and get rid of any data that is out-of-date?
  - Think about how long you really need to keep the information
- Do you **pass personal data on** to other people or organisations such as the MSA, website providers or online entry systems?
  - Is this covered in your **privacy notice** to your customers and what steps do you take to ensure it is passed on securely (passwords and encryption etc)?

Key links

The **Information Commissioner's Office (ICO)** has a lot of useful information. There is a very detailed guide to GDPR on the ICO website **HERE**, although it is over 116 pages. Perhaps start with the ICO's '12 steps to take now' by clicking **HERE**. The ICO also has a dedicated helpline for small organisations on 0303 123 1113.

This may be the beginning of a GDPR journey for your club but you can now show that you have begun the process in a structured way and with improvements all the time.

CHAPTER 2: TERMINOLOGY AND PRINCIPLES OF DATA PROTECTION

Continuing the journey to GDPR compliance, we would like to help you understand some of the key terminology associated with GDPR and also the six principles of data protection, as detailed in Article 5 of GDPR.

What terminology do we need to know?

Just like motor sport, data protection has its fair share of jargon. It is helpful to understand as much terminology as possible but these are some of the key terms you are likely to come across:

- **Personal data:** a wide-ranging term meaning **any information** relating to an identifiable person who can be directly or indirectly identified
- **Sensitive personal data:** a special category of personal data needing extra care, including race, religion, sexual orientation, genetic and biometric data. Importantly for our clubs, it includes all medical data
- **Controller:** the organisation that sets the purposes and means of processing personal data
- **Processor:** an organisation that processes personal data on behalf of a controller
- **Data subject:** any individual whose personal data or sensitive personal data you process.

Your club is a data controller but you might also be outsourcing processes, such as online entries. If so, make sure that the provider of these processing services gives you with a robust GDPR statement of its own; GDPR places specific legal obligations on processors, such as being required to maintain records of personal data and processing activities. You are **not relieved of your obligations** where a processor is involved – GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

What are the six principles of data protection?

Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject (Lawfulness, Fairness and Transparency)
    - This principle is explained in more detail in chapter three
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Purpose Limitation)
    - Tell your members what you will use their information for, and don't use it for other reasons
3. Adequate, relevant and limited to what is necessary in relation to the purposes (Data Minimisation)
    - Only collect the minimum amount of information that you really need to process
4. Accurate and, where necessary, kept up to date (Accuracy)
    - The less you collect, the easier it will be to keep it accurate and up-to-date
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (Storage Limitation)
    - Think about how long you really need to keep information, so that you can identify retention periods
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Integrity and Confidentiality).
    - How and where is the information stored, are laptops or USB sticks encrypted, and has your club got simple rules about who can access and use data?

The Information Commissioner's Office (ICO) website has more detailed guidance.

CHAPTER 3: LAWFUL, FAIR AND TRANSPARENT PROCESSING

We are going to dig a little deeper into how to process information lawfully. The key thing to remember about GDPR is that when you process information it must be done lawfully, fairly and transparently. There are six ways that data can be processed lawfully:

1. Necessary for the **performance of a contract**
2. In compliance with a legal obligation
3. Necessary to protect vital interests of the data subject
4. In the public interest or exercising official authority
5. With the **consent** of the data subject
6. In the **legitimate interests** of the controller or a third party.

Generally for clubs, most data processing is carried out for the performance of your contract with your members, volunteers or event entrants. Condition one allows for lawful processing; when someone joins your club or enters your event, they enter into a contract with you and this requires you to process their data.

If you want to process information to send marketing material which the data subject has not asked for, or would not expect to receive as a member benefit, then you must have their consent (condition five – more on this next week).

On some occasions it may also be necessary to process data for your legitimate interests. For example in case the need to contact next of kin arises (condition six).

You need to describe how your processing is lawful, and this is best done in a privacy notice. Privacy notices are a cornerstone of any club's approach to fair and transparent processing.

What is a privacy notice?

A privacy notice is your clear and transparent **statement to your data subjects** (your club members, entrants and volunteers) outlining your commitment and approach to effective data protection. It must be **freely and easily available to your data subjects at the time you collect their information. I**t should be published on your club website as a minimum (if you have one).

What do we need to include in our privacy notice?

A privacy notice should be clear and easy to understand but must include some specific information, as follows:

- The identity and contact details of the data controller
- What data is collected
- The reason(s) for processing data and the legal basis for the processing
- The recipients of the data given by the data subject
- Whether data is transferred outside the European Economic Area (EEA)
- How long the data will be held for (or the criteria to determine retention periods)
- The data subject's rights, including the right to withdraw consent
- The right to lodge a complaint with the Information Commissioner.

Is there a template we can use for our privacy notice?

The MSA has produced a **template privacy notice** for MSA-registered clubs to adapt and use for themselves. This can be found on the MSA website by clicking **HERE**. As our clubs vary in size and complexity, it will be necessary to tailor this to your needs.

CHAPTER 4: CONSENT AND OTHER CONSIDERATIONS

In the previous chapter we looked at how your club's data processing should be lawful, fair and transparent. Most of the data processing clubs do will be necessary for the performance of a contract (between the club and its members, volunteers and competitors). Sometimes a club might want to use information about data subjects for a purpose that wasn't explained, or isn't obvious. This processing must still be **lawful**, so it will be necessary to get **consent**. Now we would like to discuss the issue of 'consent' and what it means in the context of data collection and processing.

What is consent?

Article 4 of GDPR defines consent as 'any **freely given, specific, informed and unambiguous indication** of his or her wishes by which the data subject, either by statement or by clear affirmative action, signifies agreement to personal data relating to them being processed.'

Put more simply, consent is about **transparency and fairness**. If you want to process data for an entirely different reason that isn't part of the contract with your member, then you need to be crystal clear in explaining what you want to do and ask for **consent with no strings attached**. If you want to start sending marketing emails to your database, for example, then you must have consent.

What is not consent?

Given the definition above, it must be understood that pre-ticked boxes or inactivity by a data subject do not constitute consent. Additionally, **silence is not acceptance**; consent is something that must be given, not assumed.

What about emails to our members about club activities?

If you have collected email addresses and explained that you will use them to keep members informed about the club and its events (such as sending newsletters or entry forms), then you do not need consent. These activities are part of your membership offering (performing your contract) and will be obvious to new and renewing members. The template privacy notice within last week's GDPR bulletin deals with this.

Can consent be withdrawn after it has been given?

Yes. Article 7 of the GDPR is clear that data subjects have the **right to withdraw consent** at any time, and you must let them know this **before** you get their consent.

The difficulty for you as clubs is that if you are relying on consent for some lawful processing, then you must keep accurate records of how and when the consent was obtained (including the exact words you used), plus records of whenever consent was withdrawn, and even records of when consent was reobtained (including the new words you used). So please be careful – relying on consent for processing brings with it additional obligations for your club.

What other rights do data subjects have?

We have mentioned above that individuals have the right to withdraw their consent. Individuals have other rights that you should also be aware of. In last week's GDPR bulletin we highlighted that these should be included in your privacy notice, and the template privacy notice includes a list of those rights.

The right of an individual to be given copies of the information that you hold on them is known as a **data subject access request**. When asked, you have only one month to provide the information and you cannot charge a fee anymore. Knowing that most clubs rely on the goodwill of committed volunteers for their administration, it is probable that the one-month time limit will pass very quickly if you have not got a clear process for dealing with the requests.

A common problem is that club officials and committee members are not trained to deal with a request; days can be lost simply trying to find out who should be dealing with it. Have a process, make sure everyone is aware of it and remind people about it periodically.

Individuals also have the right to ask for their information to be corrected, or even deleted altogether, although this is only relevant when there is no compelling reason for its continued processing. As a club you can only delete data that you control, including photographs or results on your club website, for example.

With the GDPR effective date (25 May) still seven weeks away, there is plenty of time for clubs to consider the issues highlighted in these GDPR Bulletins and take appropriate actions.

CHAPTER 5: SUMMARY AND WHAT TO DO NEXT

This document has introduced you to GDPR – new data protection legislation that your club will need to comply with from the effective date of 25 May. We would like to close with a summary of the main points and a reminder of the things you need to do next.

What are the highlights and reminders from the MSA bulletins?

- GDPR is new EU-wide legislation that aims to bolster data protection in all areas (Bulletin 1)
- Since your club processes personal data, it must follow GDPR (Bulletin 1)
- The UK supervisory authority is theInformation Commissioner's Office (ICO)(Bulletin 1)
- There is anonline self-assessment toolto help you decide whether your club should register with the ICO (Bulletin 1)
- There are six principles of data protection (Bulletin 2)
- There are six ways that data can be processed lawfully (Bulletin 3)
- For clubs, most data processing is carried out for the performance of your contract with your members (Bulletin 3)
- You must have a privacy notice that is freely and easily available; the MSA has produced a simple template (Bulletin 3)
- If lawful processing requires consent, it must be given freely and clearly; silence is not acceptance and consent must always be given, not assumed (Bulletin 4)
- Data subjects have the right to withdraw their consent at any time, plus other rights (Bulletin 4)

What do we need to do next?

We would like the end this document how we started; with a list of the key things your club needs to do to prepare for GDPR. As before, take some time to consider the following and fill in any gaps that you uncover:

- What personal data does your club hold about people?
  - Start by making lists of all types of information you hold: member details, vehicle information, entry information, programmes, results and volunteer details are just a few
- What do you use the data for and who controls it or uses it?
  - Try to draw up a data map showing where data is and how it flows in and our of your club
- How secure is the personal data that you hold and where is it? Think about sign-on forms and other personal data collected at your events. Is it secure? Who has access to it?
  - Write a simple guide so club officials understand what is required.
  - Start to write a procedure for how the information is handled so that you can show your security measures are appropriate for the size of your club. Think about access to PCs, laptops, tablets, USB sticks, phones and how to protect those devices, such as with passwords or even encryption
- Do you take steps to keep personal data up-to-date and get rid of any data that is out-of-date?
  - Think about how long you really need to keep the information
- Do you pass personal data on to other people or organisations such as the MSA, website providers or online entry systems?
  - Is this covered in your privacy notice to your customers and what steps do you take to ensure it is passed on securely (passwords and encryption etc)?
  - Do you have consent to carry out this activity?