# Frequently Asked Questions

After having undertaken a period of research within recreational cricket, this document is aimed at addressing the frequently asked questions from cricket Clubs, Leagues, Boards and Associations regarding the introduction of the General Data Protection Regulation (GDPR) and identifying key areas ahead of the upcoming introduction into UK data protection law. The specific nature of a query will vary depending on whether you are involved at a Club, League or Board, so in most of cases we have provided principles that will accommodate all bodies, as well as some examples.

## 1. What is the General Data Protection Regulation, how is it different to the existing UK Data Protection Act?

From the 25th of May, all organisations in the UK will be subject to the General Data Protection Regulation (GDPR), which will replace the current Data Protection Act 1998. We will also have a new Data Protection Act 2018 which adds more detail to the GDPR.

The GDPR has some similarities with the existing DPA, however the GDPR places a greater emphasis on creating transparency and accountability in relation to how organisations handle individual's personal data. GDPR will help to ensure that personal data is protected by requiring us to only keep the data we need and that the data is kept securely.

The good news is that if you have been effectively complying with the existing DPA, then you are already on your way to being GDPR compliant!

## 2. What are the key changes that GDPR brings to Data Protection Law?

**Individual Rights:** A key part of GDPR is to give individuals greater rights in relation to their data. Some of these rights were in place under the old Data Protection Act including, telling people at the point of data collection how their data will be used and to let people see what data you hold about them. These rights are kept under the GDPR (although slightly changed) and some new rights are created such as the right to have personal data erased and greater rights around 'consent',

**Documentation:** Accountability is an important part of GDPR, organisations need to demonstrate this by keeping records of why they collect data, the privacy notices they serve to the people whose data is collected, how data is shared and how long it is kept.

**Legal Basis:** GDPR does not stop you from carrying out your daily tasks such as signing members to your Club etc but it means that you need to sign up individuals in a fair, lawful and transparent way. This means that you will have to justify the processing you do using conditions in the GDPR. In many cases, you will use the condition that it is necessary for you to comply with your contract obligations or

that it is in your legitimate interests to process the data and, for things like direct marketing, you may rely on consent. You will need to ensure that you only capture the data you need.

**Privacy notices.** You will need to tell individuals how you will use the data and who you will share it with. See the definition of Privacy notice below and the sample versions provided to help you create your own.

**Consent:** Consent is harder to obtain and keep under the GDPR so you need to be mindful of this and consider whether you really need consent. Sometimes we ask for consent but what we really mean is that we want the individual to confirm they understand what will happen. Consent only works if the individual has genuine free choice. If you would do the thing regardless of consent, you shouldn't rely on consent.

**Criminal records:** Information relating to criminal offence is given extra protection under GDPR. If you need to collect or use this type of information, you may need to get some extra help.

**Breaches:** You have a duty to inform the ICO within 72 hours (including weekends or out of working hours) of being aware of a breach that poses a high risk to individuals (this is explained later in this guidance). In some circumstances, you will also need to inform the data subject.

**ICO Notifications:** Data controllers (explained in the definitions below) will need to pay the ICO a data protection fee which will help to fund their work.

# 3 Key definitions

**Personal data:** Any information that relates to a living individual person and that enables them to be identified. Some examples are: individual's name, address and email address.

**Sensitive data:** Any data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric information, health and a person's sex life or sexual orientation.

**Data processing:** Anything that you do with personal data such as keeping records, using data for communication, disclosing it or amending it.

**Data Controller:** This is the organisation that is in control of how the data will be used.

**Data Processor:** This is the organisation that will use the data on behalf of the controller but cannot make decisions on that use i.e. they are following instructions from the controller.

**Information Commissioner's Office (ICO):** An independent body which is responsible for upholding data protection rights.

**Opt-in:** Where you give an individual an opportunity to actively says 'yes' to receiving communications i.e. by ticking a box to indicate 'yes'.

**Direct marketing:** Communicating with an individual to advertise or market either a product, service or anything promotional.

**Legitimate interest:** Where you process data with a legitimate/genuine reason which can be to build the game of cricket and to encourage participation in cricket which does not harm rights and freedoms of the individual.

**Privacy notice:** This is information and an explanation that is specific to the actual data which is being collected and provides the individual with details such as your identity and how you intend to use their data and informs them of their rights. It is important that there is a privacy notice whenever data is being collected.

**Explicit consent:** This is a clear statement which leaves no room for misinterpretation. This is needed when you are processing sensitive data such as; racial or ethnic origin political views, religious beliefs, trade union membership physical/mental health condition and sexual orientation. Collection of sensitive data often requires explicit consent.

## 4 What information does GDPR apply to?

The GDPR applies to 'personal data', you can find more detail in the key definitions section above.

## 5 Will GDPR apply to my organisation?

**Yes,** GDPR applies to any organisation which collects and uses personal data. As a sports organisation membership application forms are an example of where you would gather (and, maybe, hold) personal data (names and contact details etc). It is a fundamental responsibility of every organisation to have the right procedures in place to take individuals privacy rights into consideration.

## 6 My organisation is small and collects very little personal data. Will GDPR still apply to us?

**Yes,** you may have a small scale of personal data to assess in the lead up to the 25th of May, but as you collect and use personal data you will not be excluded from being required to comply with the principles of GDPR.

# 7 What are the key things we need to consider when handling personal data to be GDPR compliant?

- You need to make sure that you tell people about who you are and what you do with their data at the point of collection – this is usually provided in a privacy notice
- You should not use personal data for any other purpose than the purpose you stated at the collection point
- Only collect personal data you genuinely need, do not collect personal data just in case it may be useful in the future
- Ensure that your handling of data (collection, storage and sharing) is done securely
- Regularly review and ensure the data you hold is accurate, up to date and still needed
- Don't keep the data for longer than it is needed

# 8 What personal information should we be keeping (or not keeping) on our laptops and records?

To fulfil your role, you may need to store personal data on your laptop for processing/administering training sessions and matches etc. Every organisation needs to make sure that when people stop volunteering/change roles that they can ask for their records back or receive confirmation that their records have been deleted.

To work out what personal information, you should be keeping or not keeping on a laptop/record it is important to consider a few points:

- Do you need to store this data and why do you need to use it?
  (for example, to administer training, fixtures or facilitate requirements for sessions).
- Can you show that you are using this personal data fairly and appropriately?
  (for example: am I using it for the correct purpose).
- What can I do to make my laptop and storage drive (cloud or hard drive) secure?
  See section 9 below.

To continue to store this personal data on a laptop you need to be aware of the risks and what to do to reduce these risks by ensuring that they are stored securely.

# 9 How should we store data securely?

To securely store personal data, you should consider a few important points:

- Who will need to have access to it?
- How long they need to be kept.
- How they will be deleted once they are no longer relevant.
- How they will be updated when they are out of date.

Where you are storing personal data on electronic equipment's such as laptops, tablets, phones, clouds and One Drives, appropriate security measures need to be taken such as encryption and password protection. Personal data on spreadsheets, databases and Word documents also need to be stored securely as well as, ensuring that the data is kept up to date. Where you are keeping personal data on paper this may be more of a high risk and needs to be adequately stored and destroyed to avoid being misplaced, stolen or getting into the wrong hands.

# 10 How should we email data securely?

If you are sending personal data around your organisation or sending emails to groups of people ensure that you use blind carbon copy (bcc). Only share personal data with people who really need to have it as part of their role in cricket. Make sure that you revisit email groups and remove people when sending personal data. If you need to email anything that is particularly sensitive, maybe you could put it in a password protected Word document attached to an email rather than in the body of the email itself.

# 11 Who can we share the data with?

You should not use or share personal data for any other purpose than the purpose you stated at the collection point (in your privacy notice). Good practice would be to have a process in place that does not allow individuals' data to be used or shared for anything other than the notice has told them.

**For example**, if your Club normally shares data with Leagues or Team Managers/coaches for administrative purposes, your Club will need to include the fact that you do this within your privacy notice and you should not use it for anything other than stated on the notice. It is possible to combine a number of administrative functions and processes into one notice.

# 12 How long should we keep data?

One of the principles under GDPR is to ensure that data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

In simple terms, you should not keep more data than you need or keep it “just in case” you will need it.

Your privacy notice should clearly state how long you will keep the data you are collecting.

A good practice would be to regularly review the data you hold to ensure that it is up to date and accurate.

**Example:** You can use the personal data from last year’s season to contact players for the next season but if the individual does not re-join in that season, then you should consider deleting their data.

# 13 What happens if people sign up but they don’t “opt in” to data sharing? How do we involve them in our Club/League?

To share data with Clubs, Leagues, Boards and associations for administration or for delivering training session you do not need individuals to “opt in”, as you will not be relying on their consent as basis to share their data. For **example,** you may need to share personal data with coaches or Club managers for administration purposes or to deliver cricket training sessions. To do this you will need clearly state this in the **‘who we will disclose your personal data to’** in the privacy notice as well as the basis that you will rely on in order to share (which will probably be for the performance of a contract with the individual or that it is in your Club’s legitimate interests).

Your organisation should not be collecting or sharing personal data for anything other than the activities of your Club. Personal data should not be used for direct marketing purposes such as cricket ticket promotions etc without getting consent – especially if you are using email or SMS to invite the individual to buy or take part.

Where you are collecting or sharing sensitive data such as medical requirements/ethnic origin, you will need to obtain the explicit consent from the individual to share this data. If the individual refuses to give you the permission to share this information, then you should not do so unless it is to protect the individual’s vital interests (e.g. if they are involved in a serious training accident).

# 14 Do we need to do anything about children in our junior membership applications forms?

A child intending to participate in the organisation will need their parent/guardian to sign them up.

# 15 What should we do if a parent/guardian refuses to give us permission to keep or share their child's medical information?

Medical information is sensitive data therefore you may need explicit consent (see Section 13 above).

If the parent/guardian has not given you the explicit consent to share or keep this information and you have no other legal basis for doing so, then you should respect the parent's / guardian's wishes.

# 16 How can we make our membership forms, Privacy notices and privacy polices compliant with GDPR?

One of the key principles of GDPR is that an organisation should only process the personal data that it needs and must be transparent about how the data will be used.

How you use an individual's data needs to be set out in the privacy notice. It is important that you are clear about what you will use the information for and have this set out in the privacy notice. We have provided an example of membership forms and privacy notices for both senior and junior members. Whilst this is specifically for Club members, the same principles will apply to forms and privacy notices required by Leagues, Boards and Associations. If you undertake other activities, you may need to add to this, this privacy notice should be made available at the point of data collection.

# 17 Do we need to appoint a Data Protection Officer?

**Under GDPR you are required to have a Data Protection Officer if –**

1) You are public authority.

2) Your main activities require large scale online behaviour tracking of individuals.

3) Your main activities consist of large scale processing of special categories such as, ethnic origin or data relating to criminal convictions and offences.

As a Club or a smaller scale organisation you are unlikely to meet the above conditions or be required to appoint a Data Protection Officer. However, it is a good idea for you to nominate someone in your organisation to be responsible for data protection compliance. It is important to familiarise yourself with GDPR related issues to improve your approach to GDPR.

## 18 Do we have to contact people already in our database to ask them if we can still contact them?

You may have noticed that some organisations have sent out various forms of communication to individuals notifying them about GDPR and asking them to refresh their consent to continue hearing from them.

As you will be communicating with your members about the specific activities and information about participation in your organisation you will need to give them a new GDPR compliant privacy notice but will only have to ask for new consent if you relied on consent as your justification for processing.

## 19 Can we put personal details in scorecards, league handbooks, on our websites etc?

If you are planning on circulating fixture cards, league handbooks and websites you need to ensure that the players involved know that you are doing this and that you will be relying on legitimate interest as a basis to do so. You should bear in mind that some individuals may be unhappy about this. It is a good idea to explain why you want to do this in your privacy notice to try to avoid them exercising their rights to object.

## 20 If someone asks to be deleted from play-cricket or scorecards what do we do?

For the purpose of keeping match records and to able to carry out our regulatory function we will need to keep some information as part of the legitimate interest of cricket (although you should remember that individuals may have rights to object). Good practice would be to delete any extra personal data, keeping their full name and match record.

# 21 What should we do if there is data breach?

The first important step is to be able to identify a data breach and create a process to deal with it.

Examples of data breaches:

- Sending an email that contains personal data to an incorrect recipient.
- Devices such as laptops/printed paper work/folders containing personal data being lost or stolen.
- Computers with Club details being accessed by someone who is authorised or being hacked.
- Cloud server, Google drive and Dropbox have built in security measures to protect files but this may not help if these become corrupt/hacked.

Not all breaches require you to notify the ICO. You are to only notify the ICO if the breach is likely to cause harm to the individuals whose personal data has been breached. In the case where a breach has occurred you must report the breach to the ICO no later than 72 hours after becoming aware of it and in some cases, inform the individuals involved.

# 22 Will Brexit effect GDPR in the UK?

**No,** the ICO has been clear that the Brexit will not affect GDPR's implementation in the UK.

# 23 What should we do if an individual request to see all the information we hold about them?

An individual can request to see a copy of all the information you hold about them, this is known as subject access request. Subject access requests are not new but under the GDPR you now have one calendar month to respond instead of 40 days and, in most cases, you cannot charge a fee. Good practice would be to have a process in place to deal with subject access requests.

## 24 What is happening with Play Cricket given how much personal data is contained within that?

We are assessing the data we hold on play-cricket and working on our systems and public facing platforms to ensure compliance with the GDPR.

## 25 Can we still share reports about players behaviour and disciplinaries and umpire or groundsman ratings?

When storing and sharing information about behaviour, disciplinary actions and umpire or groundsman ratings it is important to consider, how long you will keep this information on record (taking into account the severity of the matter). Leagues should advise Clubs that reports will be made and shared, as it is important to help regulate the sport of cricket.