General Data Protection Regulation

GDPR – An Introductory Guide for Cricket Leagues

Section

1 Introduction

The General Data Protection Regulation (**GDPR**) represents the biggest shake up in European privacy laws for 20 years and will apply in all EU Member States from 25 May 2018.

The GDPR increases the sanctions and fines that can be imposed for improper processing of personal data which, along with the reputational damage that your League, clubs and the sport as a whole may suffer, is something we should be working hard to avoid.

This Guide provides an outline of the key changes a legal entity (such as your League) needs to address in order to comply with the GDPR.

Important note. This is a summary Guide only. It does not include a full list of the things you have to do to satisfy the rules and is not legal, financial or commercial advice. It is provided merely to give you an introduction to some of the things your League must do to comply with the GDPR. The England and Wales Cricket Board (ECB) is not liable for the actions taken as a result of this Guide and you should take your own advice before making any decisions or acting on the content. The Information Commissioner has published guidance and can give you extra support.

2 The Main Changes

The changes the GDPR introduces are significant. Leagues will need to start their compliance programmes to introduce, manage and rollout these changes.

What is new in the GDPR?

Leagues should already be compliant with the Data Protection Act 1998.

The GDPR preserves most of the core rules that are imposed by the current act but there are a host of changes. To help your League prepare for the new regulation, it is helpful for you to know what is changing so that you can take the necessary steps towards compliance. Below is a table of the key changes that are likely to be relevant to Leagues:

Issue	Data Protection Act 1998	GDPR
Controller / processor	Those processing personal data do so as a controller (the organisation that decides what data are collected, the purposes it is used for and who it is shared with) or a processor (who just acts on the instructions of the controller)	
Principles	Eight principles 1 **Fair and lawful.** Fair and lawful processing 2 **Purpose limitation.** Collect for specified, and lawful purposes (and nothing incompatible) 3 **Data minimisation.** Adequate, relevant and not excessive for purposes 4 **Accuracy.** Accurate and up-to-date 5 **Retention.** Kept for no longer than necessary for purposes for which it was obtained 6 **Data subject rights.** Processed in accordance with data subject rights 7 **Security**, Technical and organisational measures to protect 8 **Transfers out of EU.** Not to a territory that is not adequate	Six principles 1 **Lawfulness, fairness and transparency.** Lawful, fair and transparent processing 2 **Purpose limitation.** Collect for specified, explicit and legitimate purposes (and nothing incompatible) 3 **Data minimisation.** Adequate, relevant and limited to what is necessary for purposes 4 **Accuracy.** Accurate and up-to-date 5 **Storage limitation.** In identifiable format for no longer than necessary (some exceptions) 6 **Integrity and confidentiality.** Kept secure plus additional obligations involving security, data subject rights and EU transfers
Accountability		Must not only comply but must be able to demonstrate you comply
Notification	Criminal offence to fail to notify unless exempt	Record keeping obligations in place of notification
Processing conditions		Additional conditions available but more restrictive

Issue	Data Protection Act 1998	GDPR
Sensitive personal data (also known as 'special categories')		Expanded to include genetic and biometric data
Criminal records information	Was included in the list of 'sensitive personal data' categories	Now in its own class and cannot be processed at all unless national law allows for it
Subject access	To be administered within 40 days (prescribed fee may be charged)	To be administered within 1 month (no fee may be charged)
Amend, automated decisions and direct marketing	Rights to rectify inaccurate data, challenge automated decisions and to object to direct marketing	
New subject rights		Right of erasure (subject to conditions)
		Right to data portability (subject to conditions)
Privacy notices		Expanded to include additional information such as retention period, the legal justification for processing and contact details for the data controller and rights to withdraw consent
		Must be concise
Children		Consent from a child for online services only valid if authorised by a parent
		Stronger 'right to erasure' than other data subjects
Consent	Must be freely given, specific and informed indication of individual's wishes by which the data subject signifies his agreement to personal data relating to him being processed	Must be freely given, specific, informed and unambiguous indication of individual's wishes given by statement or clear affirmative action. Must be able to demonstrate consent has been given
	Clear and plain language required	
		Consent requests must be separate from other matters
	Requires clear and affirmative action	Requires clear and affirmative action and no pre-ticked boxes
		Must be a genuine free choice and no detriment for refusing or withdrawing consent
		Cannot bundle consents for different processing activities
		Invalid if it is a condition to the performance of a contract
		Must be explicit consent to process sensitive personal data or if consent is

Issue	Data Protection Act 1998	GDPR
		the basis to transfer personal data outside the EU
	Can be withdrawn at any time	Can be withdrawn at any time and must tell individuals they have the right to do so
Transfers outside EU	Not allowed without certain protections	The options available are more limited
		If consent is used as the transfer basis, it must be explicit consent
Data protection impact assessment		Required for 'high risk' processing
Data protection officer		Some data controllers must appoint one and there are minimum skills and requirements for the DPO Note: The UK is still deciding when a DPO will be required. It is likely this will be included in the final UK Data Protection Bill going through Parliament
Security		Enhanced security measures (such as encryption) may be needed
Use of data processors		Contract requirements expanded
		Processors have direct obligations and liabilities
Data breaches		Must be reported to supervisory authority within 72 hours
Fines	£500,000 per breach	Two tier fine (2% of worldwide turnover or €10m / 4% of worldwide turnover or €20m) depending on nature of the breach
National laws		Can pass laws to amend certain GDPR provisions. The UK Data Protection Bill going through Parliament is likely to include UK specific requirements

3 Practicalities in Cricket

Leagues are likely to already have a number of systems, processes, procedures and a lot of documentation to comply with current data protection law. These will need to be reviewed and amended to ensure compliance with the new law. There is no need to wait for 25 May 2018 – you can start implementing changes now.

The important element is to understand what personal data your League obtains, where from, what you do with it and how you protect it (basically - understand the data flows into, around and from your League). From this – you should be able to determine what changes you will need to make to comply with the GDPR.

Examples Of Things To Consider…

What data do you obtain? You can only obtain / process personal data that you need for your League's stated purposes and not merely because it may be of interest or useful one day. Any data you obtain solely for another organisation (such as visa details for the Home Office) should not be used by your League for any other purpose.

Where do you get the data from? If you enter a person's details into play-cricket or other systems, you need to be able to demonstrate you have that person's authority to do so.

Where is data stored? Laptop hard drives and USB sticks may not be the most appropriate place; cloud services will require data processing agreements with the cloud provider and may involve transfer of data outside the EU considerations

How long do you hold data for? Holding personal data about individuals that are not playing currently or recently is unlikely to be legally justifiable

How do you communicate? Using personal email addresses to send cricket communications has been common amongst volunteers but consider the use of a cricket specific email address

Is personal data protected? You may need to step up security to ensure data is encrypted and it should only be accessible by key people on a 'need to know' basis, and deleted when no longer relevant.

Do you rely on consent for your use of personal data? In many cases, consent is unlikely to be the appropriate legal justification under GDPR and you are likely to have to consider other options

Important note. In some cases, you will be using systems that are provided and operated by the ECB (such as play-cricket). The ECB is making its own arrangements to ensure that these systems comply with the GDPR as long as they are used as expected, so these will not be a priority for your League.

4 Top 10 Tips for GDPR Compliance

1. **Nominate** someone at your League Committee to be responsible for data protection compliance.
2. **Understand** what personal data you collect and why, who you share it with, how long you need to keep it for and how you protect it. You could do this by way of an audit or a gap analysis to see how your existing regime measures up to the new requirements.
3. Make sure you can **legally justify** having each item of personal data. Consent is unlikely to be the most appropriate option going forward due to the increased conditions to obtain valid consent.
4. Amend your **privacy notices** and privacy policies to include all of the new things that must be included. Remember, also, your notices and policies must be concise and intelligible. Provide the new version to all data subjects.
5. Update your **consent** requests and separate them from other elements of your privacy notice.
6. **Encrypt** personal data in any electronic devices and when sending it to anyone electronically e.g. password protecting any spreadsheets that contain personal information
7. Make sure you can satisfy **requests for access** within a month and can comply with other rights of individuals.
8. Make sure you **maintain records** to demonstrate that you comply with the rules.
9. Make sure you **train** your volunteers to follow the new law and your processes.
10. Get **help** from the Information Commissioner's Office (www.ico.org.uk)

5 Further Reading and Support

There is a lot of information in the public domain about GDPR. Not all of it is reliable and the UK Data Protection Bill is still being debated in Parliament so there may be further changes to come. For the best help and support you should use materials and support provided by the Information Commissioner (see www.ico.org.uk). In particular you may wish to consider:

- Guide to the General Data Protection Regulation (GDPR) (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/)
- 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now (https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf)
- the Commissioner's blogs which are aimed at shattering some of the myths that surround the new legal regime (https://iconewsblog.org.uk)

The Commissioner also operates a GDPR helpline for small businesses, which you may find useful. The telephone number is 0303 123 1113, option 4.