muckle LLP

UK GDPR Guide

A Guide to The UK General Data Protection Regulation (UK GDPR) for County FAs, National League System and other Football Clubs

1. Introduction

The UK data protection regime comprises both the UK GDPR and the Data Protection Act (**DPA**) 2018.

In essence the UK GDPR sets out the broad principles of data processing and the DPA 2018 goes the extra step with detailed implementation of those principles.

As part of the FA's commitment to share knowledge and best practice across the football sector, this Guide has been created to explain the UK GDPR and DPA 2018 and how you should approach these pieces of legislation.

Each club is different and there isn't a 'one-size fits all' approach or standard list of actions that need to be undertaken to ensure compliance. This Guide covers some of the commonly asked questions and provides links to further guidance and information.

The FA works with law firm, Muckle LLP, in delivering a free legal support Helpline to all County FAs. England Football Accredited Clubs and Leagues are also able to access significantly discounted hourly rates for any assistance they may need. Muckle LLP's sports team has advised clubs from grassroots to the top of the professional game. The specialist data team at Muckle LLP can provide further information and support to you on the UK GDPR and DPA 2018. If you require further help Muckle's contact details can be found further down in this Guide.

2. Glossary of Key Terms

The UK GDPR and DPA 2018 both use specific terminology you need to familiarise yourself with and consider how they apply to your club (for example, what personal data do you hold?).

The key terms under the UK GDPR are:

Consent

Any freely given, specific, informed and unambiguous indication of a data subjects wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

Data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Controller

Means 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.

Processor

A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Data subject

A living individual/ natural person.

Personal data

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Processing

Any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Special category data

Personal data, revealing:

- racial or ethnic origin.
- political opinions.
- religious or philosophical beliefs.
- trade-union membership.
- data concerning health or sex life and sexual orientation.
- genetic data.
- biometric data.

3. Does this apply to your club?

The UK GDPR applies to all controllers and processors, so if you collect any personal data in running your club (which you definitely will do if you have any members) then the UK GDPR will apply to you.

There are no exclusions for CASCs, charities or not for profit organisations. It doesn't make a difference for example if you are structured as an unincorporated organisation or company limited by guarantee – the requirements are concerned with the data you hold and how you handle this.

4. Data Protection Principles

Under the UK GDPR the data protection principles set out the main responsibilities for organisations.

Fair, lawful and transparent processing

Personal data must be processed lawfully, fairly and in a **transparent manner** in relation to the data subject.

Purpose

Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.

Minimisation

Personal data must be adequate, relevant and **limited to what is necessary** in relation to the purposes for which those data are processed.

Accuracy

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay.

Retention

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Security

Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Accountability

The controller is responsible for, **and must be able to demonstrate**, compliance with the Data Protection Principles.

5. Controller or Processor?

It is important to know, in any given circumstances where personal data is involved, whether you are acting as the controller, as the processor or in some circumstances as joint controller. Depending on which one it is, your obligations under UK GDPR will differ. For example, in the event of a data breach it is necessary to know who has the ultimate responsibility for data protection.

As set out above, the controller is the body that determines the purpose for which personal data is to be processed. In most instances where you collect personal data, you will be acting as the controller. For County FAs this can be where you collect data from your affiliated clubs and for clubs where you collect personal data regarding your players and/or their parents.

If you are entering into third party agreements, for example with a company hosting your website, then you should enter into a written contract with them to outline the responsibilities they have as processor. These contracts will likely have to be negotiated.

6. Your Key Responsibilities as Data Controller

Communication

You will need to give people information about how and what you do with their data at the point you collect it.

Responding to subject access requests

Subject access requests (requests for copies of personal data from individuals) need to be responded to within one calendar month and generally no fee can be charged for dealing with the request.

Be aware of your liability

The maximum the ICO can fine you for a breach of the UK GDPR is the higher of either £17.5 million or 4% of your annual global turnover whichever is higher. Although it is unlikely that any breaches you commit would warrant a fine at the top of this cap, it demonstrates quite how serious the implications can be for breaching the UK GDPR and why it is important to understand where you sit in the controller/processor relationship.

Data retention

Ensure you have a clear retention policy in place. You can't keep data for longer than is necessary for the purpose for which it was collected. You also need to inform people how long you will keep their personal data and you can't keep it indefinitely.

Privacy by design

If you are planning on putting in place a new system or electronic portal, then you need to consider privacy at the outset of the planning process and all the way through or prior to adoption of a new system, not at the end as an afterthought.

Data Breaches

You need to be aware of when you need to report a data breach to the ICO and ensure that you do so within 72 hours of being aware of the data breach. You also need to be aware of when you need to report a data breach to the individual(s) concerned and ensure you do so as soon as possible.

Children

There are additional protections for children's personal data. This applies to all those under the age of 16. If you collect children's personal data then you need to make sure that your privacy policy is written in plain simple English. And if you offer an online service to children, you may need to obtain consent from the parent or guardian to process the personal data.

7. Continuing Compliance

Data protection laws are not a 'one and done' affair, they impose continuing obligations on controllers and processors alike. It is important to ensure that you are compliant with your obligations at all times. Below are some top tips to keep it that way:

7.1 Process

Understand the journey that personal data takes through your club.

You should review your club and map out:

- What personal and special category data you collect/hold.
- Where you get such data from.
- Where you send this data.
- Who you share data with (internally and externally).
- What you tell people when you have collected it.
- What your legal basis for processing is.
- Why you have this data.
- How you secure the data.
- How you dispose of the data when you no longer need it.

7.2 Awareness

Make sure that your volunteers are aware of the UK GDPR and data protection issues and that they know who to talk to if they receive a subject access request or if there is a breach

7.3 Policy

Make sure the policies and procedures you have in place help your volunteers deal with data protection issues.

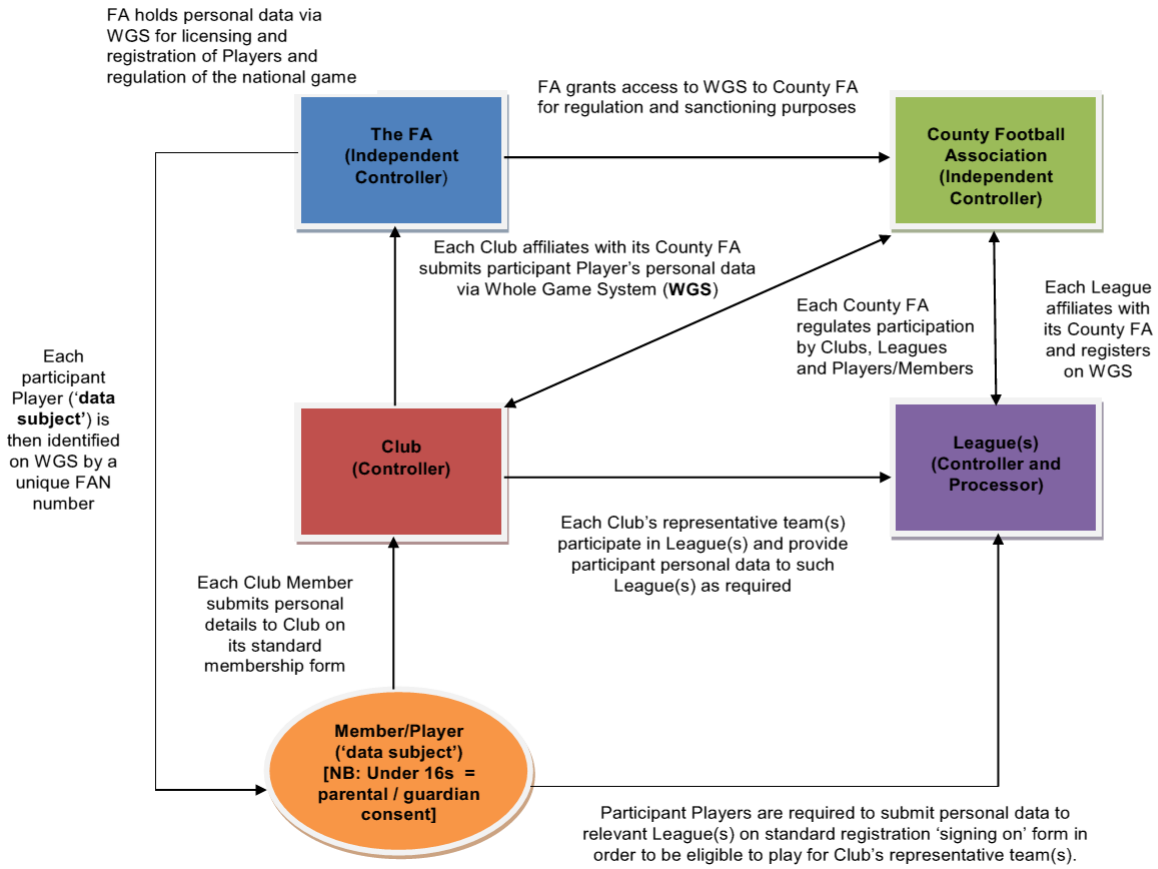
7.4 Communication

Make sure you tell individuals at the point of collection what you will do with their data and when you will delete it.

8. Data Sharing between the FA, League, Clubs and Members

Communication

As part of the process mapping to understand the journey personal data takes through your club, league or County FA you need to consider how data is transferred and shared with the FA, and other participants within the game. This will differ for all organisations but we believe that for most set-ups the basic data flow is:



9. Further Help

Muckle LLP have a series of handy factsheets you can download from the Football Association section of their website **here**.

Muckle LLP also has bite-size online training modules which can help you cut through the noise and prepare your club for UK GDPR. You can register for access **here**.

County FAs may (i) continue to use the County FA dedicated legal Helpline for any enquiries they may have and (ii) contact Muckle LLP directly to access up to 8 hours of legal support.

County FAs

Telephone: 0191 211 7798
email: Countylegalhelp@TheFA.com

England Football Accredited Clubs and Leagues are able to access significantly discounted hourly rates from Muckle LLP for any enquiries they may have.

England Football Accredited Clubs and Leagues

Telephone: 0191 211 7796
email: advice@muckle-llp.com