muckle LLP

# Data Protection

## A Guide to The General Data Protection Regulation for County FAs, National League System and other Football Clubs

# Introduction

Data protection laws are evolving. The General Data Protection Regulation (GDPR) is already in force and we are currently in a period of implementation with the deadline for compliance set for 25 May 2018.

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 GDPR and how you should approach this change in 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 achieve 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 free legal support Helplines to County FAs and Charter Standard Clubs and Leagues respectively and has sought their input in this Guide. Muckle LLP's sports team has advised clubs from grassroots to the top of the professional game, including over three quarters of the 92 professional clubs in the football league. The specialist Data Team at Muckle LLP can provide further information and support to you on the GDPR. If you require further help we have two dedicated helplines to get in touch:

**County FAs**

**Tel:** 08448 240 432
**Email:** Countylegalhelp@TheFA.com

**Chartered Standard Clubs and Leagues**

**Tel:** 0191 211 7799
**Email:** CSLegalHelp@TheFA.com

# Glossary of Key Terms

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

**Data Subject**

a living individual/ natural person.

**Personal Data**

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

Examples include: name, address, telephone number, IP address, membership numbers etc.

**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; or
- biometric data

**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.

**Data Controller**

the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws.

| | |
|---|---|
| **Data Processor** | a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. |
| **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. |

## Does this apply to your club?

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

# Main Responsibilities

| | |
|---|---|
| **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. |

# Key Changes

- **More communication**

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

- **Responding to subject access requests**

  Subject access requests (requests for copies of personal data from individuals) will need to be responded to within one calendar month rather than the current 40 calendar day period. It is also no longer possible to charge £10 for dealing with the request.

- **Obligations**

  There will be direct obligations on data processors as well as on data controllers. This may mean that if you use any third parties to process data, for example hosting your website, then you must have a written contract in place, and these are likely to be negotiated and drafted in favour of your processors.

- **Fines increase significantly**

  Currently the highest fine the ICO can levy is £500,000. Under the GDPR, from 25 May 2018, they will be able to issue fines up to €20 million euros or 4% of your global annual turnover (whichever is the higher) for serious breaches. The fine could be €10 million euros or 2% of your global annual turnover (whichever is the higher) for less serious breaches.

- **Getting consent**

  Consent will be much harder to achieve. If you rely on consent from individuals to use their personal data in certain ways, for example to send marketing emails, then there are additional requirements to comply with.

- **Data retention**

  Retention policies need to be clear. 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 whether the service provider you choose has adequate security to protect personal data.

- **Data Breaches**

  You will only have 72 hours from being aware of a data breach to report it to the ICO.

- **Children**

  There are additional protections for children's personal data. This applies to all participants 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.

## Are you ready for next year's changes?

Our top tips to start your journey to GDPR readiness are:

**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; and
- ✓ How you dispose of the data when you no longer need it.

This will allow you to identify any areas of risk.

**Awareness**

Make sure that your volunteers are aware of the 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.

**Policy**

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

**Communication**

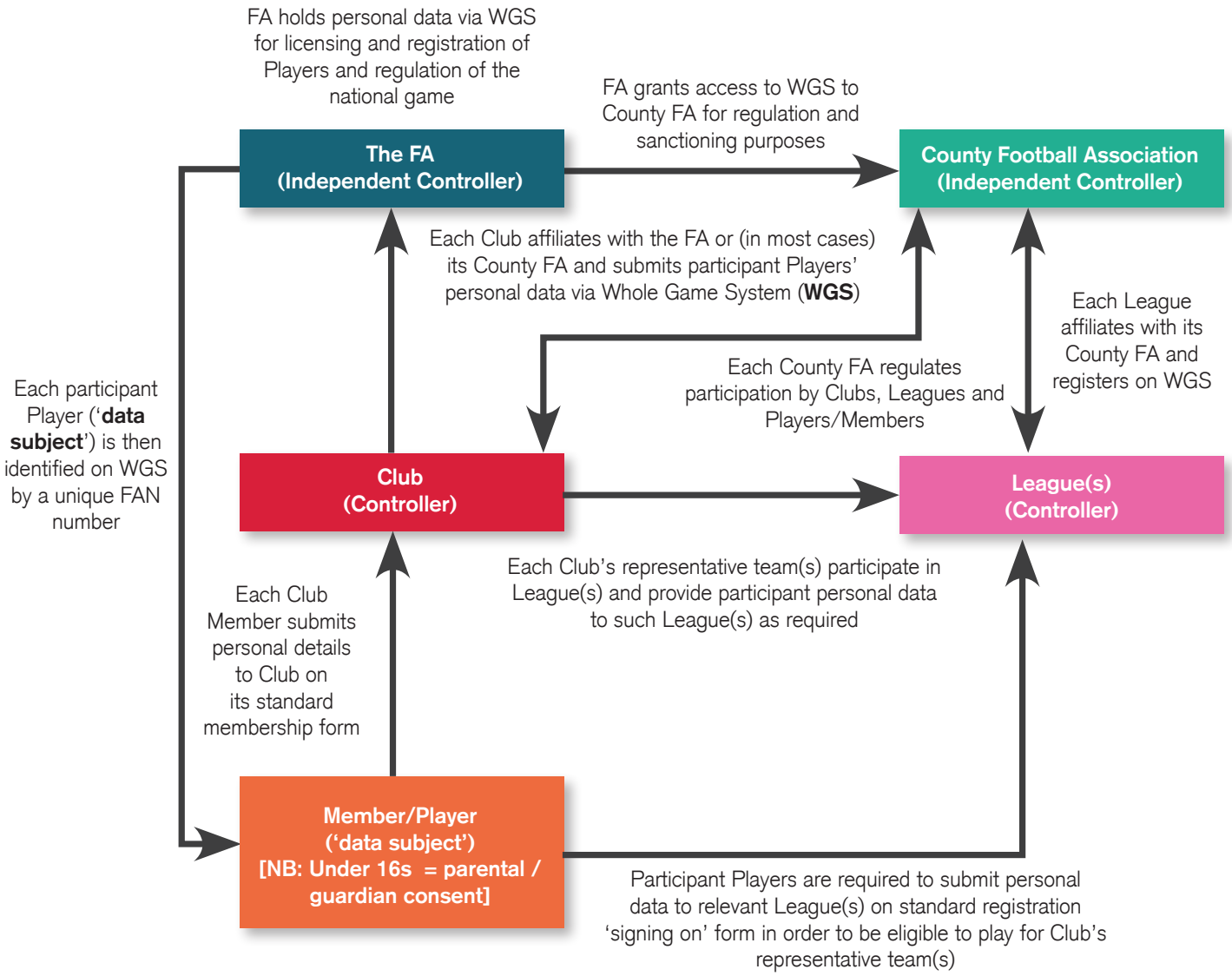
Make sure you tell individuals at the point of collection what you will do with their data and when you will delete it.

**ICO guidance**

Take a look at the 12 steps to take now and the Getting ready for the GDPR self-assessment tools on the ICO website.

# Data Sharing between the FA, League, Clubs and Members

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:



# Further Help

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

**GDPR Factsheets**

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

Charter Standard Clubs and Leagues may continue to use the dedicated Clubs and Leagues Legal helpline for up to 30 minutes free advice on GDPR enquiries (standard terms and conditions of use apply).

County FAs may (i) continue to use the County FA dedicated legal helpline for GDPR enquiries (standard terms and conditions of use apply) and (ii) contact Muckle LLP directly to access up to 5 hours' support on GDPR issues relating specifically to their organisation.

**County FAs**

**Tel:** 08448 240 432
**Email:** Countylegalhelp@TheFA.com

**Chartered Standard Clubs and Leagues**

**Tel:** 0191 211 7799
**Email:** CSLegalHelp@TheFA.com

**This Guide has been prepared based on information provided by The Football Association Limited in order to illustrate and comment in general terms only on the law and practice (as at date of publication in February 2018) relating to the General Data Protection Regulation (GDPR) which comes into force effective from 25 May 2018. However, please note that the subject matter covered is in no way exhaustive and the material does not stand on its own nor is it intended to be relied upon as a substitute for obtaining specific legal advice. The individual circumstances of each participant (County FA, League or Club) will differ. The information contained in this publication is given in good faith but any liability of The Football Association Limited or its professional advisers (including Muckle LLP) or their respective members and/or employees to you or any third party which may arise out of the reliance by you or any other party of the contents of this publication is hereby excluded to the fullest extent permitted by law. The Football Association Limited, its professional advisers (including Muckle LLP) and their respective members and/or employees accept no duty of care or liability for any loss occasioned, whether caused by negligence or otherwise, to any person acting or refraining from actions as a result of any material in this publication. We would strongly recommend that you consult professional advisers on specific issues before acting or refraining from action on any of the contents of this publication.**

muckle LLP

Pro Bono Awards 2017: Best Contribution by a Firm with an English Regional Head Office

Heart of the Community Award
Tyneside and Northumberland

Top North East dealmaker since 2014

**Muckle LLP**

Time Central, 32 Gallowgate, Newcastle upon Tyne, NE1 4BF | DX 61011

Tel: 0191 211 7777 | Fax: 0191 211 7788 | www.muckle-llp.com

Certificate No. EMS 558231