A Guide to GDPR for Clubs

This document is provided as guidance and not legal opinion. Should the reader require any further detail it is recommended that they initially look online at the Information Commissioner's Office (ICO) website (ico.org.uk) or contact a GDPR expert

What is it?

GDPR stands for General Data Protection Regulation and the EU enforced these laws across the 28 member states from 25 May 2018.

It outlines the privacy rights of every EU citizen and the ways in which an individual's 'Personal Data' can and can't be used. Personal data is information about an individual such as name, address, phone number etc. and includes special categories of personal data including one's race, ethnicity, religion or sexual orientation.

Why is it such a big deal?

Failure to comply with the GDPR will result in the risk of incurring massive fines ranging from €10m to €20m or 2% to 4% of an organisation's total worldwide annual turnover in the preceding financial year (depending on whichever is greater).

Why does this affect me or my club?

The law puts the onus on the person or entity that collects a person's information (Data Controller), to comply with the legislation and to demonstrate compliance.

Most of the Data Protection procedures should already be in place by your club and league as the Data Protection Act has been in place since 1998 but there are several keys changes that must be highlighted. The Information Commissioner's Office has published a 12 Step Guide which is worth a read.

What are the key points?

1 GDPR sets out rules about how personal Information (data) can be obtained, how it can be used and how it is stored. Sports clubs often collect the data of its members and athletes via membership forms, DBS checks, training camp applications, text or messaging systems, email list or distribution groups, training attendance lists and information captured on websites.

2 Should a member consent to the holding of his or her data, this must be communicated to them at the time the data is obtained. Even if consent is the most appropriate legal basis for processing, under GDPR the standard for obtaining consent is higher than it was previously. Agreement has to be demonstrated by clear, affirmative action, so pre-ticked boxes or opt- outs will not be GDPR compliant. A single box tick will not suffice for multiple purposes ie three separate boxes should be offered to request consent to use one's information in the following practical example: i) using training facilities, ii) signing up for fund raising and iii) getting updates.

3 Clubs must explain to members the legal basis for the use of the data. There are many legal grounds for using personal data such as 'performance of contract' and the 'legitimate interest' of the data controller. If relying on the member's consent to use data, it should be easy for an individual to withdraw their consent. The chance to review their consent should be given on a regular basis (eg yearly).

4 Data must be kept safe and secure and must be kept accurate and up to date.

5 An Individual can request a copy of all of the personal information held about them (this is called a Subject Access Request) and must be allowed to have all of their data deleted or returned to them, if they so wish, within a month.

6 Each club should consider the appointment of a Data Protection Officer (DPO) or identify someone to manage the requirements of the role. The DPO will advise on the GDPR, monitor compliance and represent the club on engagement with the Data Protection Commissioner.

What should you be doing?

Become Accountable

It is up to the club to make an inventory of all the data they have of their members and to maintain a record of what they do with this data, this is called 'data processing'. The object is to find out why, where and how the data is stored? Also, why was it originally gathered, how long it is being retained, how secure it is and whether it is shared with any third parties?

So, all paper forms, emails and computer files should be checked, updated and irrelevant data should be deleted. Data Controllers must be able to demonstrate that consent was given or another lawful grounds for processing can be relied upon and an audit trail is maintained.

Clubs will have their own systems in place for example excel spreadsheets or use third party providers to manage their digital systems. Third party providers must be well aware of GDPR compliance and discussions should be held with third parties in relation to responsibilities arising and where liability for a failure to comply will rest.

Assess your policies regarding children's data

If your club works with children, you need to scrutinise your current policies to make sure they are up to the GDPR's exacting standards, designed to protect the data of the most vulnerable among us. The GDPR's rules require the consent of a parent or guardian to record and process children's data, as well as other rules. Look at the new policies to make sure that your organisation takes children's data protection seriously.

Children under the age of 13 can never, themselves, give consent to the processing of their personal data in relation to online services.

For children between the ages of 13-15 (inclusive) the general rule is that if an organisation seeks consent to process their personal data then parental consent must be obtained, unless the relevant individual member States legislates to reduce the age threshold – although the threshold can never drop below 13 years of age.

Children aged 16 or older may give consent for the processing of their personal data themselves.

The controller is required to make 'reasonable efforts' to verify that consent has been given or authorised by the holder of parental responsibility in light of available responsibility.

Update Forms

If relying on consent, it must be 'freely given specific, informed and unambiguous'. In order to comply with GDPR, membership (or any other) forms should include the following information…

- The club identity
- The reasons for collecting the information
- The uses it will be put to
- Who it will be shared with
- If it's going to be transferred outside the EU
- The legal basis for processing the information
- How long it will be retained for
- The right of members to complain
- Whether it will be used for automated decision making
- Other specific personal privacy rights relevant under GDPR.

Personal Privacy Rights

As a data controller your club must protect the rights of individuals. They include the right to have information erased, inaccuracies corrected and the ability to object to direct marketing.

Data Portability

This is the process where an individual's information is gathered and moved to another provider or to the individual in a technical format. This is more relevant to switching banks or utility services but could crop up when an athlete transfers club or is a member of several clubs.

Data Breach

If there is unauthorised access to personal data or it is lost or stolen, the Data Protection Commissioner must be informed within 72 hours. Where there is a high risk to the rights and freedoms of the individual affected, he or she should also be made aware of the breach.

Brexit Ramifications

Clubs may be concerned over the effect of Brexit on data protection. It is expected that when the UK formally leaves the EU in 2019 it will have enacted legislation that mirrors GDPR. However, this remains to be seen.

In summary….

- Consent needs to be obtained and refreshed regularly
- Privacy statements need to be updated
- Information needs to be protected and accurate
- Specific locations of information must be known
- Subject Access Requests must be facilitated within 1 month
- Breaches must be reported within 72 hours
- Privacy by design and by default must be adopted
- New procedures must be implemented to enable the above throughout the lifecycle of the data (Capture, Store, Use, Destroy).

GDPR Action Checklist - things you should be doing

	Action	Evidence/Action completed	When	By who
1	Spread awareness of GDPR within club			
2	Ensure Privacy by design and default eg when adopting new processes and developing new systems or programmes, consideration must be given to any impact on the privacy of individuals and privacy features must be built in to new products and services.			
3	Create Inventory of data processing activities – look at points at which your club or league collects personal data. – This will help you to identify any compliance gaps or vulnerabilities and will form the basis of the mandatory record of data processing that must be maintained by most organisations under the GDPR			
4	Review situations where you are currently asking for consent and consider whether you should continue to do so or whether another legal basis, such as legitimate interest or legal obligation better fit the situation. If consent is still required, you need to ensure it meets the higher standard under GDPR and that individuals have the option to withdraw their consent if they wish.			
5	Review access to Personal Information -			
6	Review Polices and Procedures – review data protection policies including privacy notices and language you use to make sure they are at least GDPR compliant			
7	Evaluate who has access to personal data and ensure they are authorised			
8	Review and update your club's handling of children's data			
9	Evaluate any other systems that hold member information for appropriate access			
10	Ensure any third parties have provided assurance on GDPR compliance and that liability for non-compliance has been agreed – you will need to ensure that you have written agreement within the processor, that the processor gives you sufficient guarantees regarding its compliance with the GDPR			

11	Ensure paper forms are stored in known and safe locations			
12	Ensure any laptops holding data are encrypted			
13	Ensure any spreadsheets are password protected			
14	Ensure a Subject Access Request process is in place			
15	Ensure a process to report data breaches is in place			
16	Ensure appropriate documentation is in place			
17	Ensure BCC function on email is used—never reveal addresses in group emails			
18	Use cloud-based system like Microsoft OneDrive as a mechanism to keep electronic data secure			

Glossary of Terms

Consent – Freely given, specific, informed and unambiguous indication of the data subject's wishes by a statement or clear affirmative action

Data Controller – Entity which determines the purpose and means of the processing of personal data

Data Processor - Entity which processes personal data on behalf of the controller

Data Protection Officer – A person who is given formal responsibility for data protection compliance within an organisation

Data Subject – the individual to whom the personal data relates

Direct Marketing – The communication (by whatever means) of any advertising or marketing material which is directed to particular individuals

ICO – Information Commissioner's Office (UK's independent authority responsible for enforcing GDPR)

Legal Basis – legal basis for ordinary personal data includes processing in the basis of:

- Necessity for the purpose of a contract (or to enter into one)
- Compliance with a legal obligation
- Legitimate interests of the data controller
- Necessity for performance of a task carried out in the public interest
- In order to protect the vital interests of the data subject or of another natural person
- Consent

Personal Data – Any information relating to an identified or identifiable natural person

Personal 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

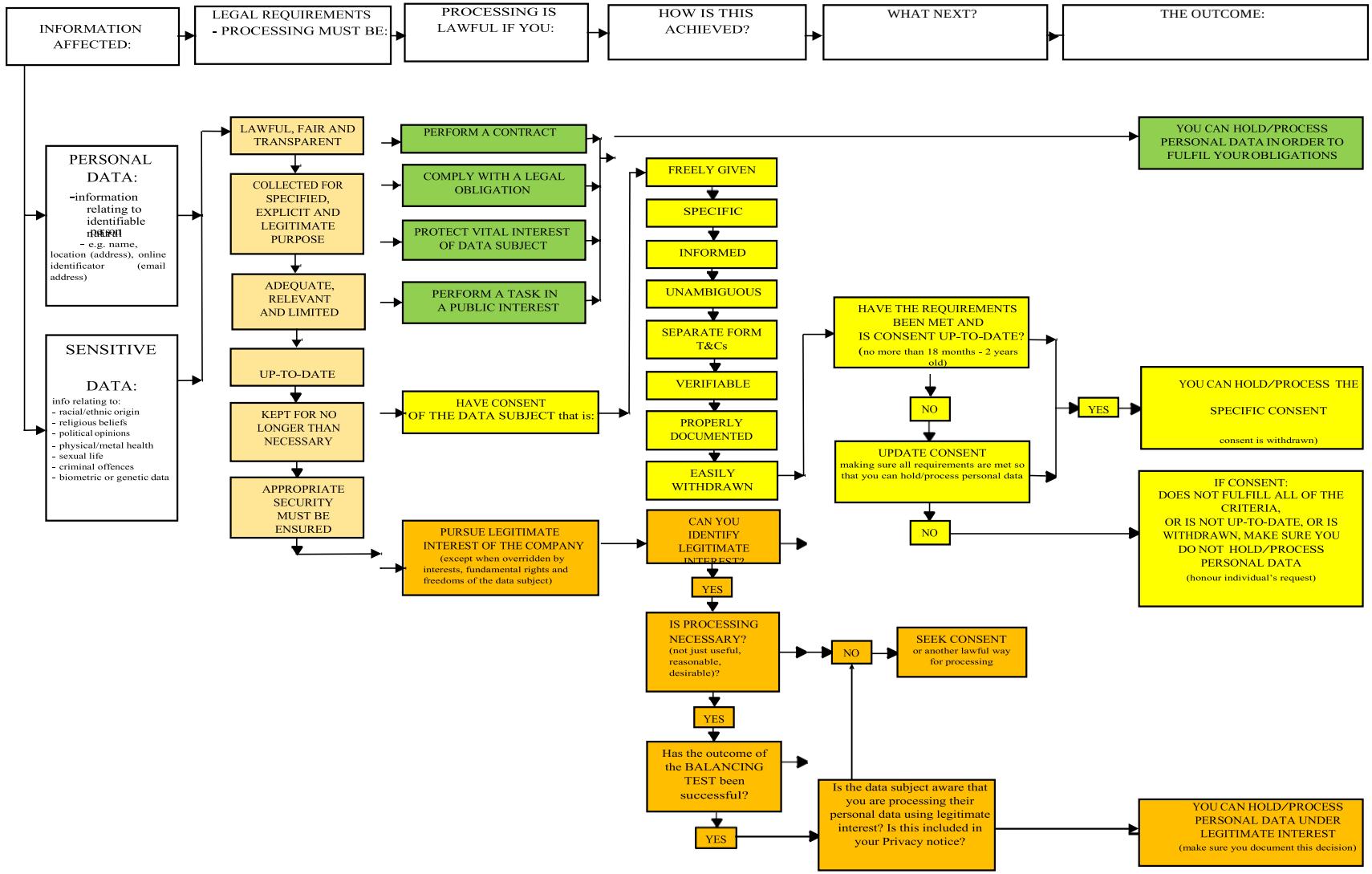
Processing – Any operation performed on personal data ….. such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – Any form of automated processing consisting of the use of personal data to evaluate certain personal aspects relating to a natural person (e.g. behaviour, personal preferences, location etc)

Pseudonymisation of data – The technique of processing personal data in such a way that it can no longer be attributed to a specific data subject.

Soft Opt-in – A mechanism by which organisations can market to existing customers on an opt out basis (subject to certain conditions being met)

FLOW CHART 1: LEGAL OBLIGATIONS UNDER THE GDPR



FLOW CHART 2: DATA YOU ARE LIKELY TO HOLD/PROCESS