



Football Supporters' Federation: guidance for supporter groups on the General Data Protection Regulation (GDPR)

The GDPR is an EU law which is coming into force on 25th May 2018. The legal landscape is very complex both because of Brexit, and the fact that there is also a UK Data Protection Bill 2017 going through Parliament which is expected to become the Data Protection Act 2018, also in May 2018, which will replace the existing Data Protection Act (DPA).

The GDPR and new DPA are much longer and more complex than existing legislation, hence the general levels of apparent 'panic' in bigger more complex organisations.

But don't panic! If a supporter organisation is currently doing things right, then there is little to worry about. This is because supporter organisations are simple organisations which people join voluntarily for a clear and quite limited purpose, and the fundamental principles are essentially the same as the current DPA.

The message is simply keep calm and carry on. If you are not doing things quite right, then this is a good opportunity to rectify things, but that should be relatively easy to do.

You need to identify someone who is responsible for this within your group. GDPR defines a controller who controls and processors, who maintain, manipulate and use personal data. These are likely to be the officers such as a secretary, treasurer and membership secretary if you have one.

Personal data is any information you keep about someone which can identify them. In practice this may well be restricted to a fan group's membership database. Processing is using that information in any way.

GDPR sets out six principles for data processing:

- It must be **processed fairly** and in a transparent manner.
- The information collected, stored and used must be for a **specified purpose**.
- It must only be used in a way that are **relevant to that purpose**.
- It must be **accurate and kept up to date**, and where found to be inaccurate is erased or rectified "without delay".
- It must **not be kept for longer than is necessary** for the specified purpose.
- You must ensure **appropriate security** to guard against loss or unauthorised or unlawful processing.

There are also six categories of lawful processing, but it's likely only two will mainly concern supporter organisations.

First, that you have the consent of the data subject for how you intend to use their personal data, and sixth, that the processing is necessary for the legitimate interests of the controller (i.e. your supporter group).

Both of these should be straightforward for a supporters organisation. For example, you can't pass on personal data of your members to say a commercial organisation without the explicit consent of everyone whose data you are passing on.

Your supporter group must keep a simple record of what items of personal data you hold, and how you use them, including policies on whether you pass them on to other organisations (unlikely) and retention policy.

You should also be aware of the rights of the data subjects, most likely your members. In very brief summary these are (i) to be informed about how you are using their data (ii) to have access to it (iii) to have it corrected if wrong (iv) to have it erased (v) to restrict certain types of processing (vi) portability (not likely to be relevant) (vii) to object to certain types of processing (viii) to object to automated decision-making or profiling (not likely to be relevant).

That's a very brief summary as things stand – however it could be subject to change as the new Act goes through Parliament. If in any doubt consult the [Information Commissioners website](#).

Malcolm Clarke
Football Supporters' Federation chair & Information Rights Tribunal member
2nd February 2018