muckle LLP

UK GDPR FAQs

What do I have to tell people when I collect their information?

Under UK GDPR there is now a fair amount of information that needs to be provided at the point of data capture in the spirit of transparency, which is detailed in our Privacy Notices Factsheet.

You have to ensure you are explaining clearly and fully exactly what is going to happen with their personal data, and why you process it. This means what you will do with their data, where will it be stored, when you will delete it.

You also have to tell them what rights they have in regards to their own personal data, which are:

- the right to access the data you hold on them;
- the right to correct any incorrect details;
- the right to have their personal data deleted (subject to exemptions);
- the right to have that data shared with another party in an electronic format ('data portability');
- the right to withdraw their consent to processing, where the legal basis for that processing is consent;
- and the right to complain to the ICO.

Data subjects also have the right to object to certain kinds of processing at any time, including direct marketing, without this objection having a detrimental effect on any other service provided or their relationship otherwise with the club or the FA.

You will also need to explain that you, the club, are the controller of their personal data, responsible for its lawful processing. You also need to set out what that lawful basis for each processing activity is, and explain which third parties you share their information with, if any.

You also need to explain that if they don't provide their details, you might not be able to process their registration to the club.

What are the legal bases on which clubs process personal data and special categories of personal data (i.e. health records)?

For any individuals and players registering with a club and the FA, then the legal basis for processing this data will be necessary for the performance of a contract, for the administration of their registration, and membership to the FA. If they are signing up to play, then to enable the arrangement of games, it is likely you will need their contact details to fulfil your part of the agreement, as the organisers.

For any emails about events or match updates you need to send, you will have the legitimate interest of keeping the members and players informed, which you will need to explain in your **Privacy Notice**.

For any staff personal data, your legal basis is necessary for the performance of a contract, for administering their pay, other employment obligations. For volunteers, the legal basis for processing their contact information is also for performance of a contract.

Any marketing emails you should have an active consent from each data subject you send marketing to. This includes passing details to third party marketers – you can only do this if you have active consent from each individual. (And if this consent is withdrawn, marketing must cease.)

Health records are classed as a special category of personal data under UK GDPR. Processing of special category data is prohibited under UK GDPR unless one of 10 exceptions applies. If the condition applying requires a basis in law then additional conditions will apply. This means that as well as needing to prove there is a lawful basis for processing you need to be able to apply one of the 10 exceptions and potentially a further requirement under the Data Protection Act 2018. For more insight to the reasons special category data can be collected, see the **factsheet on the Legal Basis for Processing**.

Health records are classed as a special category of personal data under UK GDPR. Processing of special category data is prohibited under UK GDPR unless one of 10 conditions applies. If the condition applying requires a basis in law then additional conditions will apply. This means that as well as needing to prove there is a lawful basis for processing (please refer to the **factsheet on the Lawful Basis for Processing**) you also need to be able to apply one of the **10 conditions set out on the ICO's website** and potentially a further requirement under the **Data Protection Act 2018** dependant on which condition you are reliant upon.

If you have any types of data for any other purposes, then you will need to assess why you have this data. If you don't have a valid reason for processing it, then you should think about deleting it. Full guidance on lawful bases is on the **ICO website**.

How long should I keep information for?

The official guidance is that data that can identify the data subject should be stored for no longer than is necessary for the purposes it is being processed. There are specified exemptions but only for certain research or statistical purposes. This means that once a player leaves the club or otherwise ends his membership with the FA, then personal data collected for the purposes of notifying them of matches or team news should be deleted.

You should have a clear, and it can be very simple, retention policy that staff or volunteers who deal with personal data are aware of. The guidance does not specify exactly how long this should be, but it should be reasonable and proportionate.

There are exceptions to this to be aware of.

If any investigations are pending, then you may have a legitimate interest to store it for longer until this is complete.

Staff payment data is generally kept for seven years for tax reasons.

Some bits of data may need to be kept for longer. For example, written contracts may need to be stored for a certain amount of years after the contract ends, so while you may have one copy of a player's contract filed in a secure location, there is no reason to keep this contact information elsewhere, i.e. on a database.

Insurers may also impose certain document retention periods, so you should check any existing or potential policies for this when determining you retention procedures.

What about the information I put on Whole Game System – what do I need to tell individuals about that?

As part of your fair processing or privacy notice at the point you collect the data, you should tell the individuals you will be entering their data into Whole Game System, and that this means you will be sharing it with the County FA and league. You should tell them why you're doing this. If this is not strictly necessary for their registration then they can object to you doing this. You should also point them to the privacy policy for Whole Game System.

What sort of security do we need to have?

Whatever security you have in place, or will be putting in place, needs to be proportionate to both your organisation and the risk that is posed by a breach of the personal data that you collect. There is no one-size fits all approach that can be taken, but the ICO have worked with the National Cyber Security Centre to provide a useful guide when assessing the measures appropriate for your club. **Click here**.

However you secure your data, you need to make sure that it can be accessed within a reasonable time frame, as if a player asks to see the data that you have collected on them you need to be able to provide them with this. If your data is kept in a locked filing cabinet, who has access and what contingency plans are there for accessing the data if they are unreachable? If it is kept in password protected databases (e.g. an excel document), again who knows the password to access this?

Only authorised (and appropriate) staff or volunteers should have ways of accessing personal data and should be aware of who this can be and when it should be shared. If you are processing data via a cloud hosting memory service, or on the internet, then you need to have good quality and routinely updated anti-virus and security software.

Authorised staff and volunteers with access to personal data should also be aware of their duty to keep this information confidential, and you should train these staff and volunteers to be aware that wherever they are collecting or processing personal data they must be taking care to keep it secure and confidential.

How do I find out if any of the information we have is stored overseas?

This will probably only apply if you are using a cloud hosting system. If you do, then ask your provider for information on hosting.

We use Microsoft outlook for our emails – can we still do that?

Yes. Microsoft outlook as your email provider are processors of some of your organisation's personal data, and you may also share player personal data via this platform. The UK GDPR does state that data controllers (the clubs) must have written contracts with their processors. When you purchase a Microsoft product, their standard terms and conditions form part of this written contract (even though you may never have actually read them!) and they will have updated these terms and conditions to ensure their data processing clause is UK GDPR compliant.

If you are using another organisation or individual's Microsoft subscription then you should fix this so that the club has their own purchase agreement with Microsoft.

Can I still post match information on the website?

You should be careful what information you post on a publicly accessible platform. Information that does not include personal data is fine, but players' and referees' names, strip numbers or contact information shouldn't be being posted publicly without the players' or referees' consent. You could consider posting this information behind a secure, login only members' area, but you would still need to carefully consider what data you were sharing there and why.

What do we do if there is a personal data breach?

Personal data breaches do happen, and it doesn't automatically mean you'll be in trouble with the ICO. You do have to tell the ICO within 72 hours of someone in the club first becoming aware of the breach, if the breach concerns a large amount of data, or is likely to cause harm or distress to the data subjects affected. If in doubt, get legal advice or call the ICO directly.

All staff and volunteers should be trained on what a data breach in your club might look like (for example a cyber attack, or a list of names and addresses being left in a public place) and know when and who to report it to.

Can I share members' contact information with volunteers?

Anyone who is processing personal data should be committed to an obligation of confidentiality. This means you can share data with volunteers, so long as they are aware of their responsibility to keep any data they access confidential; they use it only for the purpose they're given it; and, they follow procedures to keep it secure, and delete it when they cease to be a volunteer with you.