



Find out about the General Data Protection Regulation (GDPR) and what your club will need to do to comply with the Law.

This short guide will give you an introduction to the General Data Protection Regulation (GDPR) and the first steps that you need to take to ensure that your club is GDPR compliant and help you find more information.

GDPR will be replacing the Data Protection Act 1998 and will become enforceable in the UK on 25 May 2018.

All Archery clubs, counties & regions will need to comply with the regulations or penalties could be imposed, including very big fines. GDPR will apply to you whether you pay staff or are all volunteers, whether you have a club house or not, whether you have 10 members or 1000 members..... there are no exemptions!

GDPR is already here and the period from now up to 25 May 2018 is for implementing any changes that organisations need to make to become 'GDPR compliant'.

Regardless of Brexit; the legislation will remain enforceable

What is GDPR and why change from the Data Protection Act 1998?

Changes to data protection regulations are needed as technology has advanced. Personal data is now processed (collected, stored, shared, etc.) in different and more sophisticated ways and this new technology needed to be included.

GDPR will give EU* citizens more control over how their personal data is used. It will make it clearer for organisations (including both businesses and clubs) to understand their data protection requirements. However, it will also bring very hefty fines for those who ignore or break the rules – up to 20million euros can be levied.

How will it affect my club?

The reason that all clubs need to comply is that clubs collect data about its members – name, address, e-mail address, telephone number etc. For some clubs additional data may be collected such as date of birth, gender, emergency contact details or medical information (i.e. knowing that someone has an allergy).



First Steps to ensure that you are 'GDPR compliant'

These are the first steps that you need to take to check out what you do as a club with the data you hold:

- 1) Consider what data you hold: who holds it and who has access to it?
- 2) Consider where that data came from: how is it up-dated?
- 3) How regularly it is up-dated, how long you hold it for, do you need to hold it?
- 4) Could you use the Archery GB membership system to manage your club and not hold any information separately?
- 5) Consider what you do with the data: who you give it to, do you transfer it to other people/organisations, such as county, region and Archery GB?
- 6) Consider the security of data: where do you hold data, what data do you encrypt/password protect?
- 7) Do you have permissions from your members to do what you do with their data, when was that permission (consent) given?
- 8) Do you have a data protection policy and privacy policy, is it adhered to, is it current?

GDPR in more detail and how it may affect you and your club

When a club member joins or renews their membership and provides their details to a club, the member is also registered by the club with the relevant county, region, and Archery GB. which means that the club transfers the member's personal data to these organisations, whether this is by post or electronic means. It is therefore vital that members of clubs are told about this when they join or renew their membership.

To assist in the process for ensuring that both the club and the associated organisations comply with the GDPR in this respect, we have prepared some wording to be included on your application / membership form which we have set out below.

Proposed wording for clubs when registering members with Archery GB

"When you become a member of or renew your membership with [insert name of club] you will automatically be registered as a member of Archery GB and the relevant County and

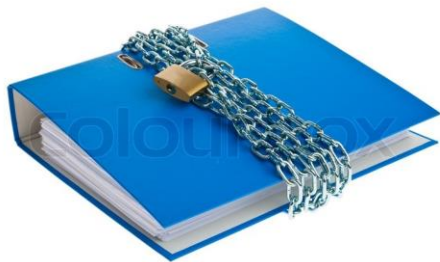
Region. We will provide Archery GB with your personal data which they will use to enable access to an online portal for you (<https://aqb.sport80.com>) which, amongst other things, allows you to set and amend your privacy settings. If you have any questions about the continuing privacy of your personal data when it is shared with Archery GB, please contact gdpr@archerygb.org.”

An example of suggested consent boxes is shown below:

“Would you like to continue to hear from us (Archery GB) about our latest news including our quarterly magazine, ways in which you can support us and membership benefits available? If so, please tick below to let us know how you would like to hear from us and confirm you contact details:

- | | | |
|--|---------|--------|
| 1) Magazine | Yes [] | No [] |
| 2) Email Newsletter | Yes [] | No [] |
| 3) Membership benefits / offers by email | Yes [] | No [] |

We will keep your details safe, and you can unsubscribe or change your preferences at <https://aqb.sport80.com> “



Frequently Asked Questions

What is GDPR and what does it mean for clubs?

GDPR is an important change in government legislation regarding data protection and stands for the General Data Protection Regulation. It effectively provides an update to the Data Protection Act 1988, bringing in new requirements and increasing the penalties for breaches. Any organisation that is required by law to comply with GDPR must do so by the 25 May 2018 at the latest.

That may sound like a long way off but there are some key changes that will affect grassroots clubs, counties and regions which need to be addressed.

Does this apply to our club?

The GDPR applies to any “data controllers” or “data processors”. Those are technical terms but, in essence, if you collect any personal data in running your club (which you will do if you have any members) then the GDPR will apply to you.

My club is only a small one with a few members: surely this won't apply to me?

Although the risk is lower, if you collect and store any personal data you will have to manage the data in accordance with strong data protection principles.

What are the key things to consider for clubs?

The principles of data protection still exist. All clubs need to ensure that with regard to personal data:

- 1) They process it securely
- 2) It is updated regularly and accurately
- 3) It is limited to what the club needs
- 4) It is used only for the purpose for which it is collected and only used for marketing purposes if the individual has given the club consent to do so.

What if my club organises events, do we need to add anything to the entry form?

Yes, as data regarding an archer's results may be passed to other organisations to publish, or be published by the organising club, the individual entering the event needs to be aware of this. Therefore, if you organise an event, to comply with GDPR, Tournament Organisers should include the following wording on tournament entry forms:

"When you enter competitions the following information may be collected and shared with tournament organisers, scoring systems and other competitors for example target lists and results may be published: First Name, Surname, Gender, Bow style, Date of Birth / Age category, Email, Address, Phone number, Club (and ID), County (and ID), Region (and ID), Round (unless defined by age), Disabled (Y/N), Disability info."

I looked at the impact of the existing UK Data Protection Act on my club and am happy that my club is compliant, so what is new about GDPR?

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

In addition to passing data to Archery GB, and the associated Counties and Regions the use of data is likely to include some of the following activities and more:

Training and competition entry

- 1) Share data with club coaches or officials to administer training sessions
- 2) Share data with club team managers to enter events
- 3) Share data with facility providers to manage access to the field & tournament entries
- 4) Share data with leagues, county associations (and county schools' associations) and other competition providers for entry to events

Funding and reporting purposes

- 1) Anonymised data shared with a funding partner as condition of grant funding e.g. Local Authority
- 2) Anonymised data analysed to monitor club trends

Membership and club management

- 1) Processing of membership forms and payments
- 2) Share data with committee members to provide information about club activities, membership renewals or invitation to social events
- 3) Publishing of competition results
- 4) Website management

Marketing and communications (where separate consent is provided)

- 1) Sending information about promotions and offers from sponsors
- 2) Sending a club newsletter
- 3) Sending information about selling club kit, merchandise or fundraising

All clubs should already have a privacy statement and policy, and certainly will need one now. This outlines to an individual who is providing you with data, details of exactly how it will be used. If someone is not clear and you do not manage data in accordance with the policy, you are increasing the risk of breaching data protection laws. Please find a link here to the [Archery GB Privacy](#) policy that can be adapted for your club.

Do I have to notify the ICO?

You no longer have to notify the Information Commissioners Office (ICO) as a data controller - you may already not need to under the current exemptions available to a not-for profit organisation.

What about Subject Access Requests?

Subject Access Requests (requests for copies of personal data from individual club members) 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. Individuals usually make requests if they have something to complain about. Make sure you keep a log of how and when you respond.

Who is responsible if we use a third party to supply our website / tournament entry system or membership system?

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. Please contact us should you require example clauses at gdpr@archerygb.org.

Could we be fined?

Currently the highest fine the ICO can levy is £500,000. Under the GDPR 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. Obviously, these fines are designed to ensure larger commercial organisations comply, but penalties exist for all sizes of organisation. The more members you have the greater the risk.

How do we get consent?

Consent will be much harder to achieve. If you currently rely on one consent opt in from an individual to use their personal data in certain ways, for example to send marketing information by email, post and SMS, under the new regulations you will now be required to use one opt in box for each type of communication.

How long should we keep data for?

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 will also need to inform people how long you will keep their personal data and you can't keep it indefinitely. For example, a member may not have renewed for 5 years- how likely is it that they will return? If the answer, is 'unlikely' then their core data should be deleted, or their record anonymised after that time.

I've heard the phrase "Privacy by design" how does that affect us?

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. Consider using the Archery GB membership system to manage your club and not hold data separately. The Archery GB system has been launched to offer improved services to clubs to help where we will be able to assure security is in place.

What happens if we discover a breach?

You will only have 72 hours from being aware of a breach to report it to the ICO. Under the Data Protection Act there are no obligations to report breaches.

For example, if a membership secretary holds the membership data on their laptop and it is not encrypted and gets stolen- the data is now at risk and a breach would have to be reported to the ICO.

You need to make sure that personal data is held securely, i.e. that electronic documents are encrypted, and password protected and that they are backed up on a regular basis.

You also need to make sure that your volunteers can identify when a breach has happened and that they know what they should do and who they should talk to.

You should consider if you need to have a separate system to the membership system provided by Archery GB.

We have kids in our club, do we have to do anything different for them?

There are additional protections for children's personal data. 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.

A local builder wants to sponsor our club house, can we give him a list of our members?

One of the principles of the Data Protection Act 1998 (and the GDPR), is that you can only process data for the purpose for which it is collected. This means that if you collect a name and contact details of an individual, so that they can become a member of your club, you can't simply use that information to allow other bodies (e.g. a club sponsor) to contact them for marketing purposes. You also need to tell people when they join your club if you are

going to transfer their data, for example to an umbrella organisation, such as your county, region and Archery GB.

What do we need to tell our members?

When individuals provide you with their details, make sure you are clear and transparent about why you have it and what you will do with their information. This means you need to make sure that you have the right data capture statements to present to individuals when they give you their personal details, and they are freely available, such as on your website.

Does all this only apply to data that is held digitally, e.g. on a computer, or does it cover paper records?

GDPR covers both Electronic and paper records. Use this as an opportunity to review filing systems and to limit the amount of paperwork you have to manage. Personal data collected manually and stored in files as a hard copy still has to be managed in accordance with the data protection regulations.

As you can imagine, some of the legislation is more difficult to implement in relation to paper copies. For example, Privacy of data is key to the GDPR. Paper documents can get into the wrong hands easily and this could easily become a data breach. Transportation of data in any format (including paper) should be seen as a threat to information security. One small slip and it's too late – an individual leaves sensitive paperwork on a train, a courier loses an archive box full of payment records, a member of a committee has files stolen from their car. These are all real-world situations where paper documents can get into the wrong hands.

We keep our membership records “in the Cloud” (e.g. via shared files on DropBox or Google Drive, or via a bespoke or commercially available membership system): what should I do about that data?

Data security is key and when storing anything online you need to ensure that you protect yourself by ensuring you keep passwords safe and ensure that files that contain personal data are encrypted. The likes of Dropbox, OneDrive and Google Drive have built in security measures for the protection of files whilst in storage or in the process of being shared. When using third party software you need to ask for assurances over the security of the system. For example, ask the provider for an explanation of how data security is managed or ask if a Privacy Impact Assessment has been undertaken. You also need to consider, how you might revoke access, when individuals change roles or leave your club.



Here are a few suggestions to help you get started towards compliance with the GDPR.

Process –

- 1) Understand the journey that personal data takes through your club.
- 2) What information do you collect, and do you need that information?
- 3) What do you tell people when you collect it?
- 4) On what legal basis have you collected it?
- 5) Where and how do you store that data?
- 6) What do you do with it?
- 7) When is it deleted?

This will allow you to identify any areas of risk.

Awareness –

- 1) 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 –

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

Communication

- 1) 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

- 1) Take a look at the [Getting ready for the GDPR](#) self-assessment tools and guidance.
- 2) The ICO also now offer a helpline. Representatives of small organisations should dial 0303 123 1113 and select option 4 to be diverted to staff who can offer support.

Archery GB advice-

- 1) if you have any questions about GDPR then please email gdpr@archerygb.org. We will monitor the queries on a weekly basis and look to respond with updated FAQs.