

Important guidance for clubs for compliance with GDPR

Information has been emailed to all clubs regarding this. If your club has not received this information or if you have any questions about the proposed wording or any of the changes under the GDPR please do not hesitate to email dataprotection@englandathletics.org.

When a club member joins or renews his/her membership and provides their details to an EA affiliated club, the member is also registered by the club with EA, which means that the club transfers the member's personal data to EA (i.e. via the Portal). It is therefore vital that members of affiliated clubs are told about this when they join or renew their membership. If your club does not automatically register all members with EA then the position changes slightly (as set out in this letter).

To assist in the process for ensuring that both the club and England Athletics 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. Please note that we are also updating our online system so that when you enter data for new members you will be required to confirm that they have been made aware that their information will be shared with EA as well.

Proposed wording for clubs who register all members with EA

"When you become a member of or renew your membership with [insert name of club] you will automatically be registered as a member of England Athletics. We will provide England Athletics with your personal data which they will use to enable access to an online portal for you (called myAthletics). England Athletics will contact you to invite you to sign into and update your MyAthletics portal (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 England Athletics, please contact dataprotection@englandathletics.org."

Proposed wording for clubs who do not register all members with EA

"When you become a member of or renew your membership with [insert name of club] you can also choose to be registered as a member of England Athletics (you will have to register with England Athletics if you ever compete for the club in competition Under UKA Rules). If you tick the box below we will provide England Athletics with your personal data which they will use to enable access to an online portal for you (called myAthletics). England Athletics will contact you to invite you to sign into and update your MyAthletics portal (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 England Athletics, please contact dataprotection@englandathletics.org."

If you do not tick the box below and then decide to compete for the club, we will need to register you with England Athletics and we will inform you at that time.
[include appropriate tick box]."

Templates for clubs to use

1. Privacy statement

We have developed a draft privacy statement for clubs to use on their membership forms or registration process. This has been approved by our legal advisors. Each club will have to insert the name of the club and amend certain sections according to how the club operates. This should provide a useful guide or if you already have a privacy statement in place it will allow you to check that you are including the most important sections.

- [Click here to download the Policy Statement](#) (PDF 32kB)

2. Membership forms

We have developed two membership form templates, incorporating the privacy statement . This will show how to apply the privacy statement in practice and inform you of the key information that is required. There is one membership form for each of the following scenarios:

- [Click here if your club registers all athletes with England Athletics](#) (PDF 802kB)
- [Click here if your club does not register all athletes with England Athletics](#) (PDF 80kB)

Please note: We have developed these templates as a guide, they are not mandatory and you may have your own in place already. They will hopefully help to clarify what is required. Please make sure you read the rest of the guidance below.

3. The GDPR Framework.

This document can be downloaded for your own use and completed so it is applicable for your organisation and how you operate. This framework will act as step by step guide and checklist covering the following -

- Map how your data is collected, stored, transferred and retained
- List all data processing activities you undertake
- Record why the data processing exists
- Identifies risks
- List third- parties that data is shared with
- Provides templates to record ongoing data protection activity

[Click here to download the GDPR Framework Register - XLS 912K](#)

4. GDPR Subject Access Request Form

The GDPR Subject Access Request process is a template that can be used to manage the process of Subject Access Requests.

[Click Here to download the GDPR Subject Access Request Process - Word 304K](#)

Frequently Asked Questions

What is GDPR and what does it mean for grassroots 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, 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 25th May 2018 at the latest.

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 grassroots clubs?

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

- they process it securely
- it is updated regularly and accurately
- it is limited to what the club needs
- it is used only for the purpose for which it is collected and
- used of 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 booking form?

Yes, as data regarding an athletes results will be passed to other organisations to publish, the individual entering the event needs to be aware of this. Therefore, if you organise an event, to comply with the Data Protection Act, race organisers should include the following wording on race entry forms:

"You agree that we may publish your Personal Information as part of the results of the Event and may pass such information to the governing body or any affiliated organisation for the purpose of insurance, licences or for publishing results either for the event alone or combined with or compared to other events. Results may include (but not be limited to) name, any club affiliation, race times, occupation and age category."

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?

More communication

You will need to tell people about how and what you do with their data at the point you collect it. For example, the purposes of clarity EA have introduced the concept of 'Athletics Data' (see definition below) that can and will be used for the administration of the sport. We have listed the activities where the data may be used and the organisations with which the data can be shared. In becoming a member of EA, EA will collect certain information about you which will include your name, date of birth, gender, URN number, email address, address, telephone number, names of the EA affiliated clubs that you are a member of and details of any coaching or officiating licenses you hold (**Athletics Data**).

You could also use this definition of data as it is likely that the same information could be used in the administration of your club. This should be included within your privacy policy.

In addition to passing data to EA (see information sent to clubs or you can request to receive it again by emailing dataprotection@englandathletics.org) the use of data is likely to include the following activities and more:

Training and competition entry

- Share data with club coaches or officials to administer training sessions
- Share data with club team managers to enter events
- Share data with facility providers to manage access to the track or check delivery standards
- Share data with leagues, county associations (and county schools' associations) and other competition providers for entry in events

Funding and reporting purposes

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

Membership and club management

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

Marketing and communications (where separate consent is provided)

- Sending information about promotions and offers from sponsors
- Sending club newsletter
- Sending information about selling club kit, merchandise or fundraising

A copy of the Draft EA Privacy Statement and Policy can be found at www.englandathletics.org/privacy-statement and www.englandathletics.org/privacy-policy. 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 isn't clear and you do not manage data in accordance with the policy, you are increasing the risk of breaching data protection laws.

ICO notifications

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.

Responding to 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. They are often contentious. Individuals usually make requests if they have something to complain about. Make sure you keep a log of how and when you respond.

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. A link to the contract clauses that EA use can be found at www.englandathletics.org/data-processor-contract-example.

Fines increase significantly

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.

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. For example, if you currently have one opt in box to 'marketing information by email, post and SMS' under the new regulations 'email, post, SMS' would have to be separated out.

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. For example, a member may not have renewed for 4 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.

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. EA is currently assessing our systems with the aim of offering improved services to clubs to help where we will be able to assure security is in place.

Breaches

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. 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.

Children

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.

Data transfer

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.

Privacy or data capture statements

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.

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

This may be a good 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 committee has files stolen from their car. These are all real-world situations where paper documents can get into the wrong hands.

My club keeps its 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.

Top tips to start your journey to GDPR readiness

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

1. **Process** - understand the journey that personal data takes through your club. What information do you collect and do you need that information? What do you tell people when you collect it? On what legal basis have you collected it? Where and how do you store that data? What do you do with it? When is it deleted? This will allow you to identify any areas of risk.
2. **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.
3. **Policy** – make sure the policies and procedures you have in place help your volunteers deal with data protection issues.
4. **Communication** – make sure you tell individuals at the point of collection what you will do with their data and when you will delete it.
5. **ICO guidance** – take a look at the [12 steps to take now](#) and the [Getting ready for the GDPR](#) self-assessment tools. 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.
6. **Muckle legal advice** – All affiliated clubs have access to a designated helpline for 30 minutes of free legal advice on any club matter including data protection. **Please note the helpline of 0845 050 8458 and email of englandathletics@muckle-llp.com are only for use by club representatives requiring assistance on club matters.**
7. **England Athletics advice** - if you have any questions about GDPR then please email dataprotection@englandathletics.org . We will monitor the queries on a weekly basis and look to respond with updated FAQs.

The guidance given here is aimed at assisting England Athletics affiliated clubs and associations with identifying the key areas that they should be addressing as a result of the additional requirements arising from the upcoming introduction of GDPR. Clubs and associations will no doubt already have considered - and where appropriate have taken specialist advice – regarding the impact of existing UK Data Protection legislation insofar as that may impact their activities. It

is similarly recommended that clubs and associations take appropriate advice if they have concerns or are still in doubt regarding specific issues having read this FAQs document. There are some suggestions within this document as to where that advice may be sought, but those should not be viewed as exclusive.