**General Data Protection Frequently Asked Questions**

**What is GDPR and what does it mean for grassroots clubs?**
GDPR is an important change in 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.

There are some key changes that will affect grassroots clubs and 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 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
- it is used for marketing purposes only 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 athlete's 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:

"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. (This is in fact already a requirement under the Data Protection Act 1996 but GDPR makes the requirement clearer).

For example, for the purposes of clarity EB have introduced the concept of 'EB 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 EB, EB will collect certain information about you which will include your name, date of birth, gender, email address, address, telephone number, names of the EB affiliated clubs that you are a member of and details of any coaching or officiating licenses you hold (**Boxing 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 EB (see information sent to clubs or you can request to receive it again by emailing dataprotection@englandboxing.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 gym or check delivery standards
- Share data on the Matchmaking data base to match bouts and enter event

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 bout 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 EB Privacy Statement and Policy can be found at http://www.abae.co.uk/aba/index.cfm/linkservid/4E589E1C-0844-F4E0-6ABDE7C4E07A3F66/showMeta/0/ . 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**
From May 25th, 2018 organisations who are processing personal data as a data controller will have to pay the Information Commissioners Office (ICO) a fee, unless they are exempt from doing so (this replaces the notification procedure under the Data Protection Act 1998). Membership organisations are likely to be exempt as long as they are not-for-profit, but you should confirm your own position to your own satisfaction (see the ICO guidance at https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf).

**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, requiring them to have appropriate security measures in place to safeguard the personal data they are processing on your behalf. Bear in mind that contract negotiations might be affected by these requirements, and processors may try to negotiate or vary terms in favour of their own commercial position. A link to the contract clauses that EB use can be found at http://www.abae.co.uk/aba/index.cfm/linkservid/4E4BF86F-DB93-3A6B-59F8ABEF20E19895/showMeta/0/

**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 certain categories of breaches. The fine could be 10 million euros or 2% of your global annual turnover (whichever is the higher) for remaining 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. You should not rely on pre-ticked boxes, nor should you assume or infer that someone has given consent, as GDPR makes clear that consent must be specific and unambiguous.

**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 3 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. EB 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 becoming aware of a 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") to reporting it to the ICO (unless the breach is "unlikely to result in a risk to the rights and freedoms of the data subjects") . Under the Data Protection Act there are no legal 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 be likely to 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.

**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, as a general rule, 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. **England Boxing advice** - if you have any questions about GDPR then please email dataprotection@englandboxing.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 Boxing 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.*