**The General Data Protection Regulation and NSRA Clubs**

The General Data Protection Regulation (GDPR) is already in force and the deadline for compliance is 25 May 2018. Although this is a European based piece of legislation it is unlikely to change as a result of leaving the European Union. There are some changes that will affect target shooting clubs that need to be addressed as the GDPR applies to any data controllers or data processors. In order to run a club you will definitely have to collect personal data about members so GDPR will apply to you.

**The fines associated with breaches of GDPR have increased significantly.** Currently the highest fine is £500,000. Under the GDPR they will be able to issue fines up to 20 million euros or 4% of the annual turnover (whichever is the higher) for serious breaches at large companies.

**Overview**

Under the new regulations, organisations must keep a thorough record of how and when an individual gives consent to store and use their personal data. Consent will mean active agreement where the individual opt in. Consent can no longer be inferred from, say, a pre-ticked box. Organisations will have to show a clear audit trail of consent. This will mean clubs and associations will have to be able to clearly demonstrate they were given permission to store and use the data – for instance, saving consent forms etc.

Individuals also have the right to withdraw consent at any time, easily and swiftly. When somebody does withdraw consent, their details must be permanently erased, and not just deleted from a mailing list. GDPR gives individuals to some degree the right to be forgotten.

People have the right to know exactly what personal data you hold, where it is located (e.g. on PCs, on servers, or in the Cloud), know that it is secure and have procedures in place to ensure its complete removal when a request to do so is made.

**Information Commissioners Office notifications**

You no longer have to notify the ICO as a data controller. However if you are currently a not-for profit organisation you probably haven’t had to so far anyway.

**Key Principles**

The GDPR provides the following basic rights for individuals; the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and rights in relation to automated decision making and profiling.

For the majority of clubs the main points to consider with regard to personal data are:

* They tell people what they are collecting
* They get their permission to do so
* They tell people who they will share it with and for what purpose
* They process it securely
* It is updated regularly and accurately
* It is limited to what the club needs
* Remove it when it’s no longer necessary
* It is used only for the purpose for which it is collected and
* Is only used of marketing purposes if the individual has given the club consent to do so.

**Communication**

You will need to give people more information and you need to tell people about how and what you do with their data at the point that you collect it. Even if you are a small club it will still apply although the risk is reduced. If you collect and store any personal data you will have to manage it in accordance with current data protection principles.

**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 (say membership), you may need to obtain consent from the parent or guardian to process the personal data.

**Getting consent**
Consent will be harder to achieve. 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. This will save effort in the future.

This could include information on:

* Name
* Address
* Date of Birth
* Gender
* Ability/disability
* Telephone numbers
* Email address
* Club/organisation affiliation details
* FAC number (if applicable)
* Club or association names
* RCO/Instructor/Coaching qualification details
* Medical issues
* Medication (for doping control or emergency)

This could be worded on application and other forms as:

*In becoming a member of (club), (club) will collect certain information about you which will include your name, address, date of birth, gender, ability/disability, telephone numbers, email address, club/organisation affiliation details, FAC number (if applicable), club or association names, RCO/Instructor/Coaching qualification details, medical issues and medication (for doping control or emergency).*

Privacy is one of the cornerstones of GDPR and privacy statements should work together with consent. Clubs and associations are encouraged to develop their own privacy policy which should include the data that is collected, what it is to be used for and any sharing that is necessary to carry out the functions of the club. Also, privacy needs to be built in at the design stage of any new systems. For example, if you are planning on putting in place a new system or electronic or otherwise, then you need to consider whether there is adequate security to protect personal data.

**Some activities where collecting data may need additional consent and privacy statements**

**Membership and club management**

Compliance with GDPR will obviously apply to processing of membership forms and payments. However, you need to be aware that data may be shared with committee members to provide information about club activities, membership renewals or invitation to social events. Also publishing of competition results, website management and sharing information with the Police needs to be considered.

**Competitions and Events**

If you organise competitions booking forms may need to be changed. This is because data regarding shooters 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 GDPR, organisers should include on entry forms something along the lines of:

*"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, selection or for publishing results either for the event alone or combined with other events. Results may include (but not be limited to) name, any club affiliation, scores and age category......"*

**Training and coaching**

You may need to inform squad or team members and coaches that you need to share data with other coaches or officials to administer training sessions. You may also need to tell them that you will need to share scores etc. with other squad coaches, selectors etc.

**Competition entry**

If you deal with competition entries you may need to inform people that you intend to share data with club team managers to enter events, share data with other clubs, leagues, county associations, uniformed groups and other competition providers for entry in events.

**Funding and reporting to funders**

Sometimes we share data with a funding partner as condition of grant funding e.g. Local Authority. If your club or association has accessed funding and individual’s data is to be shared you will need to get consent or anonymise it. It is good practice to tell people if anonymised data analysed to monitor club trends.

**Marketing and communications**

If your club or association does any marketing then there are further considerations. You may send information about promotions and offers from sponsors (say a local gun shop), sending club newsletters or sending information about selling club kit, merchandise or fundraising. These will also require consent.

**Security**

Privacy is one of the key principles of GDPR and so security is important to prevent people’s data getting into the wrong hands. If a 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) the club must make sure that data is secure. When storing anything online you need to ensure personal data is encrypted. Things like 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. If you use other software then you need to enquire about its security.

The physical security of data is also important. 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. For example, a member of committee has files stolen from their car or leaves them on a train. These are all real-world situations where paper documents can get into the wrong hands and it’s a good idea to have measures in place to prevent this.

**Keeping data**
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 5 years how likely is it that they will return? If the answer, is ‘unlikely’ then their data should be deleted on anonymised. You may also have to inform others that you have shared the data with that they should remove it.

Also people may remove their permission to collect the data and at that point it should be removed. However, you can refuse to remove the data if there were serious reasons to keep it e.g. for firearms issues, child protection or an ongoing court case.

**Changes or moving data**

Individuals are entitled to have personal data corrected if it is inaccurate or incomplete.

If you have shared data with others, you must inform them of the changes. You must also inform the individuals that you have updated the data with the other parties.

**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 organisations to contact them. You also need to tell people when they join your club if you are going to transfer their data, for example to an organisation such as the NSRA, Police etc.

You can only share data with Other organisations are GDPR compliant so make a list of NGBs, Counties etc. that you regularly converse with and make sure they are compliant

**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 then you must have a written contract in place that agrees on how the data is handled, updated, removed, secured and managed. In a club context this could be the secretary or membership secretary (data controller) allows anyone to process data (say person who hosts your website) will need to have a written document in place that agrees on how the data is used.

**Breaches**

You will only have 72 hours from being aware of a breach to report it to the ICO. Under the current 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.

**Responding to access requests**
People have the right to request access to their personal data that you keep. Subject access requests (requests for copies of personal data from individuals) 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. Normally people only make requests if they have something to complain about. For this reason make sure you keep a log of how and when you respond and that you apply any exemptions from disclosure carefully as this can e used as evidence of non-compliance.

Where requests are obviously unfounded or excessive, in particular because they are repetitive, you can:

* Charge a reasonable fee taking into account the administrative costs of providing the information; or
* Refuse to respond.

**International contacts**

If your club deals with data that is shared internationally e.g. international competitions, coaching courses etc. you’ll need to take a good look at what protections you have for international data transfers and that all parties understand the requirements of the new regulations

**Other Sections of the Regulations**

The Regulations also include controls placed on some activities which are generally beyond the scope of clubs.

* Automated decision making and Profiling**:** The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.
* Transfers: The right to data portability applies when consent is given, it is used for marketing and the process is automated