Getting Ready for GDPR

written by Neil Stevens, Data Protection Officer for the YAHR Committee
28th March 2018

What is GDPR?

GDPR stands for General Data Protection Regulation. In May 2018 we will have a new Data Protection Act which replaces the old 1998 version. It gives effect in the UK to the GDPR which is a European Regulation.

Introduction

The aim of this note is to provide an introduction to some of the concepts in the GDPR and a structure that U3As can follow as they create a data protection policy.
YAHR Committee's Data Protection Policy is available as an example of a policy which follows this structure.

What's new in GDPR?

One of the key changes are the new regulations about the way you gain consent from members to use their data:-

- Their consent must be explicit - relying on an opt out is no longer acceptable
- You must retain the evidence that members have given consent
- You need to give members more information about what you use their data for and their rights. This means that there is more emphasis on your Privacy Policy

Some Definitions

Data Controller
This is the organisation not an individual. In the case of U3As it is the Committee of Trustees. The data controller determines what data to collect how it is processed and what it is used for.

Data Processors
These are organisations that process data on behalf of the Data Controller. Processing includes the storage of data so if you use online storage like Google they are one of your data processors.

Data Protection Officer
U3As do not formally need to appoint one but it is a good idea if a single Trustee has responsibility for data protection. This person might lead a group of one or two others reporting to the main committee.

Risk Assessment
One of the jobs of the Data Controller is to consider the risks to the security of members' data. So it needs to look at all the data processors and make a judgement. Usually this means checking on the suppliers' terms and conditions or security policy.

Legitimate Interest v Consent
Organisations need a legal basis for processing individuals' information and these include legitimate interest and consent. It is important to understand the difference because if you think you need to ask for consent when you don't need to you could be creating a lot of extra work in dealing with the people who do not give consent.

a) Legitimate Interest

A U3A has a legitimate interest when it processes its members' data in order administer membership and provide the services that go with membership. Having identified your legitimate interests you need to consider whether processing data in this way is necessary to meet your objects and then balance them against the "rights and freedoms" of the individual. You should also consider whether it is a reasonable expectation of the individual that their data would be used in this way.

b) Legitimate Interests for U3As

Bearing in mind the main object of a U3A i.e. advance education of people in their third age there are services it needs to provide members to meet this object. They will include:-

- Maintaining an administrative database of its members
- Informing members of activities they can take part in
- Notifying them of its AGM
- Passing a members' email/telephone number to a group leader when that member wishes to join the group.

Would a member joining a U3A reasonably expect their data to be used in this way? Yes they would particularly as you have explained that you are using it in this way in your privacy statement.

Does the processing of their data in this way impinge on their rights and freedoms? No, but when you email people you should always give them an opportunity to unsubscribe.

What might a U3A be doing with members data that is not a legitimate interest and therefore requires explicit consent? Examples would be:-

- making a member's email/telephone number available to all the other members via a member directory on its website.
- Sending the members' name and address to the Third Age Trust for the mailing of Third Age Matters
- Emailing members information about activities that are not run by the U3A

c) Consent

In some circumstances it is not reasonable to rely on legitimate interest and for these purposes you do need explicit consent.

Recording Consent

One of the new requirements that GDPR has brought in is that members must explicitly opt-in in order to consent to you using their data in the way you describe. You should maintain a record of when and where members gave consent so that you have the evidence that they have done so. You are probably doing this already when you data capture the member's enrolment or renewal form because you know what form they filled in and when they did so.

Subject Access Request

Members have the right to ask us, in writing, for a copy of all the personal data held about them. This is known as "subject access request". One might expect this to be quite rare but you need to think how you would verify the member's id; e.g. by phoning them.

Structure

Your Data Protection Policy will include a number of different elements. Some of these might be separate documents in their own right. The main ones will be:-

Privacy Policy
This policy tells members how you are going to process their data and what you will use it for. You refer members to this policy when you collect their data. You will include an extract from it on your enrolment/renewal form.

The policy will contain sections on:-

- What data you collect
- How you use the information
- Who you share members data with
- How long you keep the information
- Members' rights to ask for a copy or have their information deleted
- How members should update their information
- Who to contact if they have a query

Your privacy policy is the public face of your data protection policy and its is usual to make it available on your website. (You can view YAHR's Privacy Policy at the bottom of our website) You would only make your whole data protection policy available if a member specifically asked for it.

Security Assessment - External
In this section you list all the organisations that process your members data and briefly note for each one what you have done to assess them and your conclusion as to the security risk. The main point is to demonstrate that you have carefully considered what happens to members' data and checked as far as you can that there is a low risk to the security of this data. This will usually be by referring to the supplier's website e.g. terms and conditions and/or statement of security measures.

Security Assessment - Internal
This section will include a brief description of how the data is handled internally and who has access to it. U3As using online systems such as Beacon will need to record who has permission to access the system and what powers these permissions grant. e.g. there will be one or two volunteers who control everyone else's access and also can download the whole data base to their own PCs; other volunteers such as Group Leaders will only be able to access details about their own groups.
There will need to be a procedure in place to keep the list of people who have access up-to-date.

Procedure in Case of a Breach
You need to record what to do if you learn there has been a breach of security; e.g. membership secretary's laptop is stolen. It is sometimes difficult to decide how and when to let members know. Your first step should be to telephone the national office who will advise you. You need to inform the Information Commissioner's Office within the first 3 days.

Training and Instructions
All volunteers who have access to data should attend a training session during which your policy and instructions for handling data are discussed.

Trustees should be taken through your data protection policy at a meeting which is formally recorded.

These training sessions will need to be once a year at least.

Other Points
You may wish to include your policy on other matters such as contact details on website.