

# Guidance Notes: Data Protection and the General Data Protection Regulation (GDPR)

These guidance notes combine both the requirements of the current Data Protection Act 1998 (DPA) and the pending General Data Protection Regulation (GDPR). The notes have been drafted to offer recommendations for the practice of U3As in respect of how U3As collect, store, use and retain the personal information of your members.

This information is general guidance and does not constitute legal advice.

## What is GDPR?

The General Data Protection Regulation (GDPR) is an update to the existing Data Protection Act 1998 (DPA). GDPR will apply in the UK from 25 May 2018 and will replace the DPA.

## What are the main changes from the DPA to the GDPR?

The main changes that affect U3As are the requirements relating to the lawful basis for processing data and accountability. There are various bases that can be used to obtain data from U3A members. These include – amongst others – legitimate interest, consent and contract. The Trust has sought legal advice on the most suitable lawful basis and the recommendation is that U3As use contract and consent. This is an update from our previous advice. Due to the payment made by members for membership of U3As this provides the necessary basis for a contractual relationship. In addition, U3As will need to gain consent from their members in relation to the distribution of the Trust publications and for sharing data outside of the U3A with organisations such as the HMRC. Where consent is gathered, U3As will need to evidence how consent has been obtained and will need to adopt an opt-in approach to gathering data.

NB: the recommendation around lawful basis is a recommendation. As independent organisations, U3As are entitled to decide that an alternative lawful basis is more suitable. The U3A needs to feel confident that it can substantiate the basis for collecting and processing the data and needs to be able to communicate this to the membership.

## What data do you currently gather?

U3As collect personal data about their members. Personal data means any information relating to an identified or identifiable natural person. This includes the information needed for membership purposes such as:

- A member's name
- Postal address
- Telephone number/s
- Email address
- Gift aid information

If there is additional information that the U3A is asking members for, the U3A needs to consider what information they are asking members to provide and why. As long as the U3A can substantiate

the basis for gathering the information and the members are aware of how their data will be processed then requirements of GDPR for gathering this information are met.

### Photographs

Photographs also constitute personal data and consent will need to be obtained for both taking and displaying photographs of the membership. Where group photographs are being taken it is sufficient for you to ask any members of the group who don't wish to be in the photograph to move out of shot.

### Special categories of personal data

Special categories of personal data are broadly the same type of data that was referred to as 'sensitive personal data' under the DPA. These include:

- the racial or ethnic origin of the individual;
- political opinions;
- religious beliefs, philosophical beliefs or other beliefs of a similar nature;
- whether he/she is a member of a trade union;
- physical or mental health or condition;
- sexual life or sexual orientation; or
- genetic data and biometric data where processed to uniquely identify an individual.

It is unlikely that U3As will be gathering special categories of personal data. However the U3A may want to consider what, if anything, the U3A needs to record in relation to an individual member's physical or mental health or condition. As detailed above, the U3A will need to substantiate the basis for requesting this information and explain this to the relevant members. The U3A would need to consider the basis for requesting this information and may need to gain consent or complete a legitimate interest assessment.

### Data Protection Principles

Article 5 of the General Data Protection Regulation revises the Data Protection Principles established by the Data Protection Act. The principles stipulate how personal data should be processed:

#### Principle 1

**Personal data must be processed lawfully, fairly, and in a transparent manner relating to individuals.**

- This principle requires U3As to:
- Inform members as to which lawful basis is being used to gather their information
- Inform members as to what their personal information will be used for
- Inform members as to how their information will be held
- Gain consent from members to communicate with them for different purposes i.e. general U3A information, specific group information

What U3As need to do:

- Review what information is currently held, where it is held and who has access to it.
- Add privacy statements to relevant paperwork where hard copy forms are used. Example forms have been drafted and are shown below:
  - Launch questionnaire
  - Membership application form
  - Renewal membership form

- Review the different ways that members are asked for their information i.e. are group conveners gathering information?
- Retain the documents (electronic or paper) that you use to gather consent as they will constitute the evidence you need to demonstrate compliance.
- Ensure that any documents are retained securely.
- Identify who members need to contact should they wish to withdraw their consent for their information to be used for certain purposes i.e. a member no longer wishes to receive the Trust magazines.
- Let members know who to contact and how to contact the person who will respond to any requests for consent to be withdrawn. You may need more than one method if you have members who are not online.
- Let members know once their request to be withdrawn from certain communications has been dealt with.

## Principle 2

**Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.**

This principle requires U3As to:

- Only use members' information for the purposes that they you have informed them of and/or they have provided consent for..
- Gain consent for transferring data outside of the U3A i.e. to a travel company for a trip

What U3As need to do:

- Be specific about what the U3A is going to be using member information for. This is detailed in the sample privacy statement.
- Avoid using members information for sending information that could be considered as 'marketing'.
- Ensure that group conveners are aware of what communications are considered 'appropriate'.
- Let members know who to contact if they feel that they have received communications that are not what they have signed up for.
- Provide a prompt and comprehensive response if members feel that they have received an inappropriate communication.
- Be aware that some members may be more sensitive than others regarding data protection due to personal experiences.
- Be as transparent as possible with how the U3A operates in relation to its communications with members.

## Principle 3

**The collection of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.**

This principle requires U3As to:

- Limit the information gathered from members to what is needed for membership purposes.

What U3As need to do:

- Consider and review on an ongoing basis what information the U3A needs and what purpose it is used for.

When investigating complaints that might require the U3A to request further personal information from a member be sure to record any meetings accurately.

#### Principle 4

**Personal data held should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.**

This principle requires U3As to:

- Keep up to date and accurate records
- Identify who on the committee is responsible for keeping information up to date

What U3As need to do:

- Ask members to keep their information up to date and let them know who they need to contact to update their information
- Use membership renewal (in whatever form the U3A currently does this) as an opportunity for members to update their personal information.

#### Principle 5

**Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.**

This principle requires U3As to:

- Archive or delete information that is no longer required for membership purposes.

What U3As need to do:

- Make a decision as to how long member information will be retained for.
- Not use member data for communication purposes beyond the period of their membership unless there is a specific and agreed need to.
- Review how data is 'deleted' and what happens to the data if it is stored on a database.
- Archive or delete (depending on how long you need to keep member information) the data of those who do not renew.
- Be aware of where the U3A needs to retain data for a longer period in order to meet any legal or statutory requirements and where this is the case inform the relevant member.

NB: for U3As who use Gift Aid you will need to keep member information in line with the timeframes specified by HMRC.

## Principle 6

**Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.**

This principle requires U3As to:

- Keep personal data and special categories of personal data secure
- Discuss and agree processing arrangements with any 3rd party suppliers such as venues, travel agents
- Consider who within the U3A Committee needs access to the full membership information and restrict access to those who need it.
- Ensure that committee members/group conveners who hold information delete or return all data when relinquishing their roles.
- Gain consent from members where information is to be passed to a 3rd party and inform members as to what information will be shared.

GDPR also requires organisations to be aware of individual's rights, which are:

- 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

What U3As need to do:

- By following the key principles as detailed within this guidance the U3A should not be infringing the rights of its members.
- Inform the membership how they can make a 'subject access request' (a request to view the data that is held on them) and how quickly this will be responded to.
- Review your practice in relation to data on an ongoing basis.
- Discuss data protection within the steering committee and provide an induction for new committee members.
- Ensure group conveners are aware of expectations in relation to data protection.
- Liaise with National Office if you encounter any issues that the U3A is unsure about or need further guidance with.
- Discuss data protection at network meetings if the U3A is a network member.
- Look to access local or national training to help with awareness.
- Adopt a data protection policy and privacy policy.

## Data security and emails

What U3As can do:

- Ensure that Committee Members use strong passwords – the recommendation is that these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols.
- Avoid sharing passwords with others

- Encourage Committee Members not to keep passwords written down somewhere where they can be easily accessed and identified
- Avoid leaving PCs with sensitive information on them in such a way that someone else could easily access that information
- When sending confidential information by email use password protection.
- Avoid opening e-mail attachments from an unknown source.
- Consider purchasing firewall software for Committee Members PCs. This can be purchased and downloaded from the internet.
- Avoid keeping written records of negative comments about U3A members or suppliers. Where there is an issue between members ensure that any recordings are factual and avoid recording opinion unless directly from an interview. For serious matters, please contact National Office for support.
- Avoid sending emails that could be considered offensive or discriminatory.
- Avoid sharing email addresses or personal information via email without permission
- If a laptop is stolen or lost that holds a large amount of member information please contact National Office.

### Accountability principle

GDPR introduces an accountability principle that requires U3As to be able to demonstrate, compliance with the data protection principles. The principle refers to a 'data controller' -however it is recommended that within U3As the committee assume joint responsibility for how data is processed and managed.

What U3As can do:

- Review the U3As current policies and data protection practice and record this formally
- Add data protection to the agenda of the U3A committee meetings and minute the meetings
- Agree that all committee members have joint responsibility for data even where it is not accessed by all members. This will help to avoid the responsibility feeling too burdensome for the membership secretary.
- Access training for committee members
- Ensure practice is transparent by adopting policies and putting statements regarding privacy on U3A paperwork and the website
- Follow through on the things that the policy says the U3A will do
- Induct new committee members and group conveners in the principles of the GDPR and how they apply in practice

### Breach notification

The GDPR will introduce a duty on all organisations to report certain types of data breaches to the relevant supervisory authority, and in some cases to the individuals affected.

What U3As need to do:

- On discovering a breach investigate the extent of the breach:
  - How many members does the breach potentially affect?
  - What personal information has been exposed?
  - How did the breach occur?
- Keep a record of actions taken since the breach was discovered and take any immediate actions needed to reduce any further breaches

- Contact National Office to discuss whether or not the Information Commissioner's Office needs to be informed of the breach. These will be reviewed on a case by case basis.
- Report serious breaches i.e. ones that could risk the rights or freedoms of individuals.
- Be aware of timelines for serious breaches as these need to be reported within 72 hours.
- Inform members, as required, if there has been a data breach providing them with full information.

#### Useful sources of further information

The Information Commissioner's Office website has useful and downloadable materials on their website. <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>