Data Protection and the General Data Protection Regulation

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 your practice in respect of how you collect, store, use and retain the personal information of your members.

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 consent and accountability. u3as will need to gain consent from their members to obtain, retain and use their personal information. u3as will also need to evidence how you are complying with the principles of data protection which includes evidencing that members provided consent.

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.

Due to the nature of the work of the u3a it is perfectly legitimate for you to request this 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 it has the member's consent for obtaining the information then requirements of GDPR for gathering this information are met. Photographs also constitute personal data and consent will need to be obtained both taking and displaying photographs of the membership.

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:

- genetic data and biometric data where processed to uniquely identify an individual. 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.
- 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 hold their information.
- Gain consent from members to communicate with them for different purposes i.e. general u3a information, specific group information.
- Inform members as to how they can withdraw consent for their information to be used.

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 outlined above, as long as the u3a can substantiate the basis for requesting this information and it gains the member's consent then the u3a is meeting the requirements of the GDPR for gathering this information.

Data Protection Principles

There are 8 data protection principles that were established under the DPA. These have been moderately revised by the GDPR. For the purpose of this guidance the focus is on what an u3a needs to do to ensure compliance.

Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner

This principle requires u3as to:

- Review what information is currently held, where it is held and who has access to it.
- There is no expectation that u3as gather consent retrospectively but they need to implement systems for this going forward.
- Consent needs to be obtained from members at the point at which they provide their information.
- Review whether there are other ways that the u3a is asking members for their information i.e. are group convenors also gathering information? Consider whether the u3a needs to review your systems for how it gathers information.
- Consent needs to be refreshed when information changes. It is also advised that consent is gathered again a on a regular basis which can be done via your membership renewal forms.
- Retain the documents 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 can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

This principle requires u3as to:

- Only use members' information for the purposes that they have provided consent for.
- Gain additional 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 convenors 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 compared to the purpose(s) data is collected for.

This principle requires u3as to:

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

What u3as need to do:

- Consider a review on an ongoing basis what information is needed 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 are erased or rectified without delay.

This principle requires u3as to:

Keep up to date and accurate records.

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 the membership renewal form as an opportunity for members to update their personal information.
- Archive or delete (depending on how long you decide 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.

Principle 5 – Personal data which is kept in a form which permits identification of individuals shall not be kept for longer than is necessary.

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.

Principle 6 - Personal data must be processed in accordance with the individuals' rights.

This principle requires u3as to:

Be aware of what an individual's rights 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 convenors 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.

Principle 7 - 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, etc.

What u3as need to do:

- Consider who within the u3a needs access to the full or partial membership information and restrict access to those who need it.
- Control who is permitted to process (create, view, change, delete, download) personal data. This may involve maintaining a list of who is allowed to do what.
- Gain consent from members where information is to be passed to a 3rd party and inform members as to what information will be shared.

Principle 8 - Personal data cannot be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data.

This principle requires u3as to:

Consider whether there are any circumstances where information would need to be transferred outside of the EU.

What u3as need to do:

- Check whether there are any third party suppliers which the u3a supplies information to who may pass member information to parties outside of the EU.
- Talk to National Office who will obtain advice if you intend to transfer any personal data outside of the UK and the EU.

Data security and emails

What u3as can do:

- Ensure that all 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 password with others.
- Encourage members not to keep passwords written down somewhere where they can be easily accessed and identified.
- Avoid leaving PCs, laptops or other devices with sensitive information on them left 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, laptops or other devices. 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.

If a PC, laptop or device is stolen or lost that holds a large amount of member information please contact National Office.

Accountability and governance

The GDPR requires organisations to be able to demonstrate that they comply with the data protection principles.

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.
- Access training for committee members and other data users.
- 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 convenors 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 has useful and downloadable materials on their website. Click here to visit

Updated 04/10/2023