General Data Protection Regulation

The General Data Protection Regulation (GDPR) will apply in the UK from 25 May 2018 replacing the Data Protection Act 1998 ("DPA"). The Government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

PERSONAL DATA AND SPECIAL CATEGORIES OF PERSONAL DATA

Personal data means any information relating to an identified or identifiable natural person: for example, names, email addresses, telephone numbers, addresses, online identifiers (such as IP addresses) and location data are all personal data. Personal data that has been pseudonymised – eg key-codes – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual. Personal data of this type should be the only type of data included in the U3A membership databases. No other information or data should be included.

"Special categories of personal data" are broadly the same types of data as "sensitive personal data" under the DPA and 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.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

PRINCIPLES

Under the GDPR, a U3A must not only comply with the Data Protection principles below – which are roughly similar to the ones included under the DPA - but it must also show how it complied with the principles (please see Section E for more details about Accountability and Governance).

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

- Processing is broadly defined and in effect will cover any activity involving personal data (such as obtaining, recording, holding, using, disclosing or erasing data).
- Lawful bases for processing personal data include: (i) receiving the consent of the individual; (ii) if the processing is necessary for the performance of a contract with the individual or to take steps to enter into a contract; or (iii) if the processing is necessary for compliance with a legal obligation. Always ensure that the members consent to be on a database to allow the U3A to contact them about U3A activities of a local, regional or national nature. You also need to ensure that you keep a record of such consent to meet the requirements of "accountability" under the GDPR.
- Before processing "special categories of personal data" about an individual (for example, entering it on a database), ensure that you have obtained the individual's explicit written consent. It is not anticipated that the collection of "special categories of personal data" will ever be required by a U3A membership database.
- Consent must be a freely given, specific, informed and an unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in. Consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and you will need to provide simple ways for people to withdraw consent.
- You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But you should review your consent mechanisms and practices to ensure that these will meet the GDPR standard on being specific, granular, clear, prominent, opted-in, properly documented and easily withdrawn, if you rely on individuals' consent to process their data.
- The GDPR contains new provisions intended to enhance the protection of children's personal data. Since a U3A does not process children's personal data, this guide does not cover such provisions.
- If you receive data from a 3rd party, please check with that 3rd party that consent was received from the individual whom the data relate to before those were sent out externally.

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.

- Only use personal data in a way that falls within an individual's reasonable expectations or stated/ consented purposes. Further processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes is not considered to be incompatible with the initial purposes.

- If you are going to use the information for any purpose that goes beyond this, such as to add names to a marketing list and/or pass on the data to a 3rd party, you must explain this clearly and obtain the specific consent of each member on the database before passing data to third parties.
- Do not send e-mails or SMS for marketing purposes without getting consent from the intended recipient.
- If a person indicates that they do not want to receive marketing communications, promptly amend the relevant database and ensure that the person's wishes are respected by notifying all internal contacts who need to know.
- Before transferring personal data outside the U3A, ensure you have obtained the individual's consent.

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.

- Collect only personal data that is necessary for the purpose in hand e.g. names, email addresses telephone numbers and addresses. Do not collect irrelevant or excessive personal data.
- When collecting information on a database, drop-down boxes and free-text boxes need to be examined carefully to avoid unnecessary personal data and "special categories of personal data" being collected.
- Do not enter negative comments on any individual, including U3A members or suppliers, onto any database.

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.

- Have processes in place to regularly check what records are kept, and to make sure you are not keeping information that is irrelevant, excessive or out of date.
- Update inaccurate information – or delete such information.

5. Personal data which is kept in a form which permits identification of individuals shall not be kept for no longer than is necessary.

- Delete information that you have no genuine business need for. As a rule of thumb, personal data about a U3A member who has left the U3A should be deleted within 6 months.
- Personal data may be stored for longer periods if the personal data is processed solely for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes. Appropriate technical and organisational measures must be

implemented to safeguard the data and the rights and freedoms of individuals.
- If you need to hold data for longer than what is necessary, hold the data in an anonymised way.
- Ensure that records which are to be disposed of are securely and effectively destroyed.

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

- Please see 'Individual Rights' below for more details. If you receive any request in respect of these rights, please forward it promptly to the Business Secretary in your U3A, and advise the Business Secretary to contact National Office for assistance.

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.

- Keep personal data and "special categories of personal data" secure (for example, keep records in a locked cabinet, use password protection and restrict access to specific U3A Executive Committee members– please see the Information Security document for more information).
- Ensure that all members comply with Section C below - Data Security Checklist.
- If a 3rd party supplier is engaged to do any of the processing on behalf of the U3A, ensure a legal review of the contract with that supplier is undertaken to ensure that the supplier agrees to act only on the U3A's instructions and to comply with specified security measures.

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.

- Always talk to National Office who will obtain advice if you intend to transfer any personal data outside of the UK and the European Union.

DATA SECURITY AND E-EMAILS CHECKLIST

- If you use a password, ensure that you use a strong password - 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.
- Always keep your password and user name secure and do not share them.
- Always lock your PC while it is unattended.
- Consider sending confidential information by secure e-mail.
- Do not open e-mail attachments from an unknown source.
- Do not to open spam – do not even unsubscribe or ask for no more mailings. Instead delete the email and either get spam filters on your computers or use an email provider that offers this service.
- Do not believe emails that appear to come from a bank that ask for account, credit card or password details (a bank would never ask for this information in this way).
- Avoid asking for sensitive personal data unless necessary for a legal or business purpose, or passing on "special categories of personal data" about somebody else.
- Do not make negative comments about any individual, including other U3A members or suppliers. If you feel that there is an issue which other people need to be aware of speak to National Office first about the next steps.
- Do not send any e-mail which might be construed as offensive or discriminatory and do not download obscene material.
- Do not download programmes or games, or run any such programmes or games sent to you by e-mail.
- Do not download business data onto any personal laptop unless authorised.
- Ensure that any personal data held on a laptop is encrypted.
- Tidy your inbox, outbox and folders regularly. Do not store messages or attachments longer than necessary.
- When taking records or laptops off-site, ensure that: (i) only the necessary information is taken; (ii) such information is controlled at all times; and (iii) U3A security advice is followed.
- If your laptop is lost or stolen, contact National Office immediately.

INDIVIDUALS' RIGHTS

The GDPR provides certain rights for individuals, which strengthens some of the rights that currently exist under the DPA.

If you receive any request in respect of the below individuals' rights, please forward it immediately to the Business Secretary in your U3A, and advise the Business Secretary to contact National Office for assistance.

1. The right to be informed:

When a U3A collects personal data, it must provide to the individual the following information (usually through a privacy notice):

- identity and contact details of the U3A (and where applicable, the U3A's representative) and the data protection officer.
- purpose of the processing and the lawful basis for the processing.
- the legitimate interests of the U3A.
- any recipient or categories of recipients of the personal data.
- details of transfers to third countries and safeguards.
- retention period or criteria used to determine the retention period.
- the existence of each of the individuals rights.
- the right to withdraw consent at any time, where relevant.
- the right to lodge a complaint with a supervisory authority.
- whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.
- if applicable, the existence of automated decision making, including profiling and information about how decisions are made and the significance and consequences of such decisions.

The information supplied must be:

- concise, transparent, intelligible and easily accessible.
- written in clear and plain language.
- free of charge.

Each U3A should review its current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

2. The right of access:

Individuals will have the right to obtain:

- confirmation that their data is being processed.
- access to their personal data – This is called a "subject access request".
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

If a "subject access request" is submitted by an individual, copy of the information must be provided free of charge – but a U3A can refuse or charge a "reasonable fee" (which must be based on the administrative cost of providing the information) for requests that are manifestly unfounded or excessive, particularly if these are repetitive.

Information must be provided without delay and at the latest within one month of receipt of the request. A U3A may be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, the U3A must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

If a U3A refuses a request, it must tell the individual why and that he/she has the right to complain to the supervisory authority and to seek a judicial remedy. A U3A must do this without undue delay and at the latest, within one month.

Each U3A should review its current procedures to work out how to react if someone asks to have access to their personal data. As previously mentioned, if you receive any such "subject access request", please forward it immediately to the Business Secretary in your U3A. You should also advise the Business Secretary to contact National Office for assistance.

3. The right to rectification:

- Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. The U3A will have one month to comply with a request for rectification (unless the request for rectification is complex, in which case this can be extended to two months).
- If a U3A has disclosed the personal data in question to 3rd parties, the U3A must inform them of the rectification where possible. The U3A must also inform the individuals about the 3rd parties to whom the data has been disclosed where appropriate.

Each U3A should review its current procedures to work out how to react if someone asks to have their personal data rectified (e.g. Would your systems help you to locate and rectify the data? Who will make the decisions about rectification or carry out the rectification?).

As previously mentioned, if you receive any such request, please forward it immediately to the Business Secretary in your U3A, advising the Business Secretary to contact National Office for assistance.

4. The right to erasure (or the "right to be forgotten"):

Individuals have a right to have their personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- When the personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- When the personal data must be erased in order to comply with a legal obligation.

There are limited grounds under which an organisation can refuse to comply with a request for erasure and these include cases where the personal data is processed: (i) to comply with a legal obligation; (ii) to exercise or defence of legal claims; or (iii) for statistical purposes.

If a U3A has disclosed the personal data in question to 3rd parties, the U3A must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

As previously mentioned, if you receive any such request, please forward it immediately to the Business Secretary in your U3A, advising the Business Secretary to contact National Office for assistance.

5. The right to restrict processing:

Individuals have a right to restrict processing of their personal data (for example when the individual contests the accuracy of the personal data).

When processing is restricted:

- A U3A is permitted to store the personal data, but not to further process it. The U3A can retain just enough information about the individual to ensure that the restriction is respected in the future.
- If a U3A has disclosed the personal data in question to 3rd parties, the U3A must inform them about the restriction on the processing of the personal data, unless it is impossible or would involve disproportionate efforts to do so.

6. The right to data portability:

This right allows individuals to move, copy or transfer their personal data easily from one IT environment to another in a safe and secure way, without hindrance as to usability.

If a request is made, a U3A must:

- Provide the personal data in a structured, commonly used and machine-readable form.
- Comply without undue delay, and within one month – unless the request is complex or the U3A receives many requests, in which case this can be extended to two months.
- Provide the information free of charge.
- If the individual requests it, transmit the data directly to the other organisation if this is technically feasible.

7. The right to object:

Individuals have the right to object to:

- a U3A processing their personal data for the performance of a legal task or the U3A's legitimate interests.
- direct marketing (including profiling).
- processing for purposes of scientific/historical research and statistics.

Although there are limited exemptions, if a U3A receives such request, it must stop processing personal data as soon as it receives an objection. This is key when it comes to marketing emails and texts.

8. Rights in relation to automated decision making and profiling.

This section only applies where the processing operations constitute automated decision making (i.e. without human intervention). Since this type of processing does not seem to apply to the way U3As process information, details have been left out of these guidance notes.

ACCOUNTABILITY AND GOVERNANCE

The GDPR requires organisations to demonstrate that they comply with the above principles.

To that end, a U3A must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that the U3A complies with its data protection obligations. This may include the review of current policies, the implementation of internal data protection policies, on-going staff training and internal audits of data held, where it came from, who it was shared with and other processing activities.
- Maintain relevant documentation on processing activities.
- Implement measures that meet the principles of data protection by design and data protection by default (i.e. designing projects, processes, products or systems with privacy in mind at the outset) to ensure that privacy and data protection are key considerations in the early stages of any project, and then throughout its lifecycle.

  Measures could include:
  - Data minimisation.
  - Restrictions relating to pseudonymisation.
  - Transparency.
  - Allowing individuals to monitor processing.
  - Creating and improving security features on an ongoing basis.
- Where appropriate, carry out data protection impact assessments to identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy.

A U3A may also:

- Appoint a Data Protection officer – Whilst this is recommended, it is unlikely to be a legal requirement to individual U3As since each U3A does not carry out large scale systematic monitoring of individuals nor does it carry out large scale processing of "special categories of personal data" or data relating to criminal convictions and offences.
- Sign-up to a code of conduct or certification scheme – The GDPR endorses the use of codes of conduct and certifications as tools for controllers and processors to demonstrate compliance with GDPR obligations applicable to their processing operations. This is not an obligatory requirement; however, if an approved code of conduct or certification scheme that covers a U3A processing activity becomes available, the U3A may wish to consider working towards it as a way of demonstrating that it complies.

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.

A U3A must notify the ICO of a breach where such breach is likely to result in a risk to the rights and freedoms of individuals or if the breach is likely to have a significant detrimental effect on individuals (for example, if it results in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage). This is assessed on a case by case basis. For example, a loss of customer data will need to be notified if the breach leaves individuals open to identity theft. However, the loss or inappropriate alteration of a staff telephone list would not normally meet this threshold.

Individuals must also be notified where a breach is likely to result in a high risk to the rights and freedoms of individuals (Note - the threshold for notifying individuals is higher than for notifying the ICO).

Breach notification must contain the following information:

- The nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned.
    - the categories and approximate number of personal data records concerned.

- The name and contact details of the data protection officer (if one has been appointed) or other contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.

- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

A notifiable breach must be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay. Failing to notify a breach when required to do so can result in a significant fine; up to 20 million Euros or 4% of a group global turnover.

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred.

If you suspect or become aware of any data breach, you need promptly inform the Business Secretary in your U3A, and advise the Business Secretary to contact National Office for assistance.