THE CENTRAL COUNCIL OF CHURCH BELL RINGERS

UK Registered Charity No. 270036

THE 2018 GENERAL DATA PROTECTION REGULATION (GDPR)

Interim guidance for CCCBR and affiliated societies based in the United Kingdom

Overview

The GDPR will be directly applicable in EU member states from 25 May 2018. It does not require national legislation to be implemented and when the UK leaves the EU, the GDPR - like other directly applicable EU legislation - will form part of the UK's domestic law under the European Union (Withdrawal) Bill. The Data Protection Bill will replace the 1998 Data Protection Act (DPA), incorporate the GDPR and the Law Enforcement Directive into UK law and deal with permitted derogations.

The GDPR is only concerned with personal data i.e. any information related to an identified or identifiable living individual. It provides a more detailed definition than the DPA 1998, making clear that information such as an online identifier can also be personal data; reflecting changes in technology and the way organisations collect information about people.

The GDPR has implications for Towers, Guilds and Association as well as the Central Council of Church Bell Ringers.

What's different

The GDPR introduces significant changes. However, the fundamentals will remain broadly the same. The definitions are similar; the concepts of data processor and controller are retained; the data protection principles still apply but have been expanded to include transparency, data minimisation and integrity; and personal data and sensitive personal data (now referred to as special category data) have been expanded to include a broader definition of personal data and two new categories of 'sensitive personal data'.

The GDPR retains the existing rights of data subjects and introduces enhanced rights including the right of 'erasure' (to be forgotten, although there can be compelling reasons to continue processing data), data portability and extended rights to object and be informed. Consent will become a restricted concept under the GDPR in that it must be freely given, specific, informed and an unambiguous indication of the data subject's wishes.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Legal basis for processing

For processing to be lawful under the GDPR, you need to identify a lawful basis. These are often referred to as the "conditions for processing" under the DPA. It is important that you determine your lawful basis for processing personal data and document this. Under the GDPR your lawful basis for processing has an effect on individuals' rights. For example, if you rely on someone's consent to process their data, they will generally have stronger rights, for example to have their data deleted.

There are six lawful bases available for processing personal data:

1. Consent of the data subject
2. Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
3. Processing is necessary for compliance with a legal obligation
4. Processing is necessary to protect the vital interests of a data subject or another person
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
6. Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

There are 10 lawful bases for processing ***special categories of data*** (i.e. data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health, sex life or sexual orientation).

Individual rights: *(Please refer to the ICO website for further details)*

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision making including profiling

What do you need to do?

If you have not yet looked into the GDPR, you should familiarise yourself in the first instance with the guidance published by the ICO. There is an updated '12 steps to take now' document and a 'getting ready for GDPR checklist' in the ICO's self-assessment toolkit (this is a useful and free resource and external consultants will often ask organisations to complete this before they advise).

https://ico.org.uk/for-organisations/charity/charities-faqs/

Over the first few months of 2018, consider moving towards GDPR compliance over three "phases":

- Phase 1 – Communication – inform association officers of the changes to the legislation and their responsibilities
- Phase 2 – Discovery. Conduct an "information audit" of personal data that your Association currently collects / processes / stores. Also look at your existing forms, consent wordings, privacy notices and the like. Document what legal bases you have for processing personal data.
- Phase 3 – Change. Devise new wordings for privacy notices and consent forms.
- Phase 4 – Embed. Ensure that your Association's policies and procedures become embedded into routine practice.

Things to think about:

- Members – If you publish members' personal data (eg name, address, email, telephone number) in your Annual Reports, newsletters or Association website, you need to have members' explicit consent. The best way to achieve this is to use an appropriately-worded opt-in consent statement on your Association's annual subscription renewal form.
- Membership database:
    - How is it stored?
    - How secure is it?
    - How do you back it up?
    - How do you ensure it is up to date?
    - What procedures do you have in the event of loss / corruption?
    - What procedures do you have in place in the event of theft or data breach?
    - What procedures do you have in place to track members' data consent?
- Other ICT considerations:
    - Database and website security – security permissions and levels of access controlled by password
    - If members' personal data is stored in the cloud, have you ascertained where in the world this storage exists?
    - Ensure anti-virus and anti-malware is robust and up to date
    - Does your Association website have a GDPR-compliant Privacy Notice?
    - Does your Association website use cookies? If so, are you compliant with "cookie law" by advising website users?
    - Does your association website use https or SSL? If your website includes any online forms, then using security certificates is highly recommended.
    - Do you have members' consent to publish their contact details on the Association website?
    - Do you obfuscate members' email addresses to prevent them being harvested?
    - When email multiple members, do you use Bcc?
    - If your Association has a social media presence you must ensure that, as data controller, you do not infringe the data protection rights of any living individual. For more information, see also the CCCBR Guidance on social media (update coming soon) - https://cccbr.org.uk/wp-content/uploads/2016/03/Social_Media_Guidance_2013.pdf
- Financial information
    - If you store members' bank account details (eg: for direct debits etc), how are you securely storing and securely disposing of that information?

- Newsletters
    - If you publish photographs of individuals in your newsletters, do you obtain their consent?
    - If you email newsletters to your members do you keep a record of when they "opted-in" to receiving the newsletter?
- Minutes of Meetings
    - Under GDPR, if people are named or referred to in minutes of meetings this is classed as personal data. Are minutes of meetings kept private and only circulated to those present? If minutes are in the public domain, do you need to seek consent from those present to publish them?
- Children
    - Children have the same rights as adults under GDPR
    - The GDPR contains new provisions intended to enhance the protection of children's personal data.
    - Where services are offered directly to a child, you must ensure that your privacy notice is written in a clear, plain way that a child will understand.
    - Unless the child is deemed "competent", a parent must grant consent for their child's data to be collected, processed and stored.
- Third parties
    - If you rely on any third parties for collecting / storing / processing personal data, have you established their GDPR compliance?

Data Breaches

A personal data breach can broadly be defined as an incident that has affected the confidentiality, integrity or availability of personal data.

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely there will be a risk, you must inform the ICO within 72 hours of the breach being discovered; if you decide you do not need to report the breach, you should still document it.

In the event of a suspected breach of the Act the following should be addressed:
- Containment and recovery;
- Assessment of ongoing risk;
- Notification of breach;
- Evaluation of response.

Top five tips

Here are the ICO's "top five" data protection tips for small and medium sized charities and third sector organisations:

1. **Tell people what you are doing with their data**
   People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice) so it is important you are open and honest with people about how their data will be used.

2. **Make sure relevant Association officers are adequately trained**
   Ensure that relevant Association officers have a clear understanding of their responsibilities in terms of how they should store and handle personal information. Refresher training should be provided at regular intervals for existing officers.

3. **Use strong passwords**
   There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep your information secure from would-be thieves.

4. **Encrypt all portable devices**
   Make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.

5. **Only keep people's information for as long as necessary**
   Make sure your Association has established retention periods in place and set up a process for deleting personal information once it is no longer required.

Further advice. Please refer to these useful sites:

http://www.parishresources.org.uk/gdpr/

http://www.cfg.org.uk/resources/Publications/cfg-publications.aspx#GDPRguide