

GDPR - General Data Protection

Regulation Q&A for PCCs

This Q&A is intended to give the **Clergy** and **PCCs** information on the new **General Data Protection Regulation (GDPR)** which comes into force on 25 May 2018.

It is designed to raise the awareness of GDPR in each Parish, to think about the personal data held and what plans and actions need to be taken to be compliant by the time the new regulation comes into law.

This Q&A is deliberately brief and everyone in the PCC should read this.

A more detailed Guide is contained in Bulletin 1A which is designed for those who will take the lead in the PCC on GDPR.

Q1. What is GDPR?

A. GDPR is a stronger Data Protection REGULATION which will supersede the existing Data Protection Act. GDPR updates the rights of individuals in a networked world and takes into account the changes in technology since the original Data Protection Act was introduced.

Q2. Does GDPR apply to PCCs?

A. Yes! Everyone who works in the parish (clergy and laity) must comply with GDPR. GDPR covers information about any living individual held by any organisation or person. As soon as a PCC/person gathers and processes (uses) information the existing Data Protection Act applies and GDPR will be no different. PCCs must be compliant with the new regulation as it will become law in 2018. Brexit has no impact as all EU laws will be adopted when Britain leaves the EU.

Q3. What is personal data?

A. Personal data means any information relating to an identified or identifiable person. A data subject, is an identifiable natural person who can be identified, directly or indirectly, by reference to identifiers such as:

- Name
- Identification number (National Insurance no or business allocated number)
- Location data (address)
- Online identifier (email address, IP address)
- Sensitive personal data (health, sexual orientation)

Q4. Do PCCs need to register with the Information Commissioner's Office? (ICO)

A. Not always, it depends on what you do with the personal data. Most organisations need to 'notify' the Information Commissioner that they process personal data. For PCCs the situation is not straightforward. The current position is that PCCs are exempt from the notification requirements if they only **collect** the following basic data:

- Electoral Roll
- Gift Aid Records
- Accounting Records
- Employee Payroll Records
- Membership lists of groups within the parish ("Friends", Mothers' Union etc)

If PCCs hold more than the simple basic data outlined above, or hold records on other matters e.g. pastoral issues; youth group or wish to mail out from the information listed above or wish to use the information for other purposes they should register.

Note: If this personal data is to be used for other purposes e.g. to publicise services, fundraising or other events then clear consent must be obtained stating what the personal data will be used for. See Q5.

Registration with the ICO can be done online and costs £35 annually. To register click here. <https://ico.org.uk/for-organisations/register/> PCCs must register with the ICO if CCTV is installed.

The ICO can also be contacted for free for advice and have on line guides to GDPR on their website which can be downloaded. <https://ico.org.uk/for-organisations/data-protection-reform/>

PCCs must comply with GDPR when it comes into force regardless of whether they have registered.

Q5. What does consent mean under GDPR?

A. According to the Regulation consent means “any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.”

In practice, this means GDPR requires PCCs to ensure that when consent to hold an individual’s personal data is obtained, it is clear, unambiguous and states clearly how long the data will be held, what it will be used for, what process is in place for the individual to contact you to gain access to their information and how they can withdraw their consent. Personal information obtained for one purpose cannot be used for another unless the consent form clearly states that is what will happen.

Q. What do we as a PCC need to do now?

A. The first thing you must do is not panic. The second is to take this seriously, there is ample time if you act now. GDPR is an enhancement and strengthening of individuals rights. It will not prevent PCCs from holding data.

Actions:

1. The first thing to do is to appoint a data compliance officer. The PCC Secretary would be a good choice, but it can be someone else such as an employee of the PCC. This person will become the “expert” for the PCC and the contact point for Subject Access Requests. The data controller is the incumbent. (In times of vacancy this role would go to the Churchwarden).
2. Put GDPR on the PCC agenda as a standing item. Progress, concerns and actions should be discussed and documented.
3. Review the personal information held.
4. Review your current consent forms and privacy notices. Do they need to change?
5. Review the existing procedures for retaining and deleting data.
6. Review the existing procedures to respond to subject access request.
7. Review how you seek, record and manage consent to hold personal data and ask - do you need to make changes?

Training Seminars

Arrangements are being made for training events to be held in the Spring and full details and how to book your place will be issued early in the New Year.

Further updates on GDPR will be issued as more information becomes available.