Colchester Deanery: General Data Protection Regulation Briefing

Current law

- Data Protection Act 1998
- Defines how an individual's personal data may be processed lawfully by organisations
- Set out 8 principles for processing of data
- Created a regulatory authority for data protection – Information Commissioners Office (ICO)
- Applies to Church as with any organisation

Key terms

- Personal Data - records which relate to a living individual – e.g. name
- Sensitive (Special) Personal Data – criminal, health, political, race, religion, trade union membership
- Processing – anything done with personal data.
- Data Subject – living individual e.g. you
- Data Controller – the organisation or body who controls data processing
- Data Processer – a third party who processes data on behalf a Data Controller

6 legal grounds for processing data.

- Data Subject consent
- Necessary for contractual obligation with Data Subject
- Necessary for legal obligation other than contract
- Necessary for vital interests of the Data Subject
- Necessary for functions of public bodies (public task)
- Necessary in the legitimate interests of Controller balanced by consideration, on a case-by-case basis, of any overriding legitimate interests of the Data Subject

8 principles

1. Processed fairly and lawfully
2. Processed only for specified and lawful purpose(s)
3. Adequate, relevant and not excessive re the purpose
4. Accurate and, where necessary, kept up-to-date
5. Not kept longer than necessary for the purpose
6. In accordance with Data Subjects' rights
7. Kept secure by technical/organisational means
8. Transferred outside EEA only if privacy protected

GDPR – new law?

- Not really new: legal grounds and 8 Principles remain, although are enhanced through accountability and transparency.
- More personal data (numbers, IP addresses)
- More sensitive personal data (biometric ID, sexual orientation)
- Enforcement more stringent

DPA vs GDPR: six principles

- Lawful, fair and transparent.
- Purpose limitation
- Minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

Protections on data transferred internationally still there but not a principle

DPA vs GDPR

- Accountability – 'super' principle, no longer simply about stating compliance, now must show how you are compliant.
- Policies and procedures will be of greater importance.
- Greater emphasis on transparency – informed – Privacy Notice.

DPA vs GDPR: consent

- Consent – 'freely given, specific, informed and unambiguous'.
- Must be affirmative. Silence, inactivity and assumed 'consent' are not consent. An end to pre ticked boxes. Also meant to be 'unbundled'.
- Data Controller must be able to evidence.
- Must also be easy to withdraw and request to withdraw can only be refused if there is a legal basis to continue processing.
- Minimum age at which consent must be given is 16, probably will be 13 (UK Bill).

Data subject rights

- access
- erasure
- rectification
- restriction
- object to processing
- data portability
- to complain
- if profiling occurs
- if further processing will occur

- Do not necessarily need to comply, but must have an overidding legal reason not to.

DPA vs GDPR: other key changes

- Subject Access Requests – no fee and shorter time for response – 1 month.
- Data breach – e.g. loss of data, must be reported to ICO within 72 hours of discovery.
- Much larger fines – max £10 m or £20 m – however they will mainly be used on serial offenders.
- Data Protection Officers required for some organisations – parishes will not need a DPO, but do need someone to take a lead.

What do we do?

- Don't panic – you do not need to be fully compliant by 25 May – but you do need to have plan.
- National Guidance http://www.parishresources.org.uk/gdpr/
- Notify your trustees – PCC members – use the two page guide.
- Identify you key 'implementers' e.g. Parish Priest, Churchwarden, PCC Secretary/Parish Administrator – use the detailed guidance.

What do we do?

- Audit your data processing using the template.
- Prepare a Privacy Notice using the audit findings – template.
- Consider consent – do you need to get further consent?
- Consider procedures – write these down.
- Consider breach procedure – write these down.

ICO website

- https://ico.org.uk/for-organisations/data-protection-reform/
- 12 steps to take now.
- Guidance for small organisations - https://ico.org.uk/for-organisations/business/
- IT Security https://ico.org.uk/for-organisations/guide-to-data-protection/it-security-top-tips/
- Checklist.

Q&A