Item 6

General Data Protection Regulations Briefing

(the presentation you've all been waiting for)

Current law

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

Key terms

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

6 legal bases 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
- 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

New law - GDPR

- Legal bases and 8 Principles remain
- More personal data
  (numbers, IP addresses)
- More sensitive personal data
  (biometric ID, sexual orientation)
- Enforcement more stringent
- Applies to Church as with any organisation

DPA vs GDPR

- Accountability – 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 – right to be informed – Fair Processing Notice

DPA vs GDPR

- Consent – must be affirmative and evidenced– silence, inactivity and assumed 'consent' are not consent. Must also be easy to withdraw and can only be refused if there is a legal basis to continue processing
- Right of erasure (aka right to be forgotten)
- Rights to restrict and object to data processing

DPA vs GDPR

- Subject Access Requests – no fee and shorter time for response
- 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.

What do we do?

- Don't panic
- Do an audit of data processing
- Remember Incumbents are separate data controllers to the PCC
- Guidance from National Church – very useful. http://www.parishresources.org.uk/gdpr/

National guidance

- Detailed guidance note, for lead,
- Summary guidance note, for PCCs,
- A checklist,
- A template for an audit,
- Guidance and sample forms for obtaining consent,
- Guidance on writing Privacy Notices and some templates.

ICO website

- https://ico.org.uk/for-organisations/data-protection-reform/
- 12 steps to take now.
- Checklist.

Training events

- Training events being arranged
- Two sessions (afternoon and evening) per Episcopal Area
- Watch out for booking invite