DIOCESE OF OXFORD

GDPR for Parishes and Deaneries

November 2018

v2.0 15NOV18 1

1

GDPR: Your area of interest

DIOCESE OF OXFORD

1. Parish
2. Benefice
3. Deanery
4. Other – charity, chaplaincy, school, etc.

2

2

GDPR: where is your parish/benefice/deanery?

DIOCESE OF OXFORD

1. Not started yet
2. At the planning stage
3. Some steps taken (for example, Privacy Notice published)
4. Most areas of parish activity are GDPR compliant
5. All areas are GDPR compliant

3

3

GDPR: Important, but don't over-react

Church Won't Name Dying Man In Prayer To Avoid Breach Of Eu-Backed Data Protection Rules

4

4

Interpreting the law

5

5

Interpreting the law

Personal data is

"information that relates to an … identifiable individual"

John Smith in St Paul's PCC?

6

6

In this session

1. About GDPR: definitions
2. GDPR: key concepts
3. Journey to Compliance

means internet search terms

7

7

About GDPR: Definitions

8

8

General Data Protection Regulation (GDPR)

Data Protection is about **avoiding harm** to **individuals** by misusing or mismanaging their personal data.

GDPR is:

1. An extension/tightening of existing data protection legislation (DPA 1998)
2. UK data protection law is now a combination of:
   - EU General Data Protection Regulation 2016/679 (the "GDPR")
   - UK Data Protection Act 2018 (the "DPA 2018")

   All generally referred to as "GDPR".

9

9

Personal Data

Personal data is any information about a living individual, which is capable of identifying that individual:

- on paper *as well as* digital/electronic
- images *as well as* text (e.g. photos, CCTV)
- don't forget *indirect*

The **Data Subject** is the person about whom personal data is being processed

Sensitive Personal data is any information relating to an individual's

- Racial or ethnic origin
- Sexual orientation
- **Religious**, political or trade union affiliation
- Genetic or biometric data

Known as '**special category**' data.

NB Christian religious affiliation can be *inferred* for church members.

10

10

Data Controllers and Processors

Data Controller

- The legal entity that decides *how* the data is *kept and used*

(the data controller may also process data, also you can have joint controllers)

Data Processor

- A different legal entity who is actually processing (using) the data, (on instructions from the data controller)

Recording, disseminating, adapting, obtaining, destroying, organising, erasing, transmitting, retrieving, combining, altering, holding … … are ALL DATA PROCESSING

Watch out for different **legal entities**: incumbents, PCCs, ODBF, ODBE, suppliers, etc.

11

11

A Glimpse of the Process…

12

12

Typical steps for parishes/deaneries:

1. Raise awareness
2. Conduct a Data Audit (and data mapping)
3. Identify (and document) your 'lawful bases'
4. Check your processes meet the 'eight rights' and 'seven principles'
5. Review how you get consent
6. Build in extra protection for children
7. Data retention and disposal
8. Review your Data Sharing
9. Update Policies & Privacy Notices
10. Work out how you will deal with Subject Access Requests
11. Data breaches: how will you detect, report and investigate?
12. Training
13. Build-in data protection to your new initiatives

rochester diocese gdpr toolkit
(simpler version at parishresources.org.uk/gdpr)

13

13

GDPR: Key Concepts

14

14

GDPR: Eight Rights of Individuals

- **Right to be Informed**
  Informed about the collection and use of their personal data (transparency)
- **Right of Access**
  (a.k.a. Subject Access Request) may be made verbally or in writing. One month to respond. No fee.
- **Right to rectification**
  Correcting inaccurate data
- **Right to erasure** (right to be forgotten)
- **Right to restrict/suppress processing**
  In certain circumstances: store data but not use it.
- **Right to Data Portability**
  Ease of movement between IT environments
- **Right to Object**
  Absolute right with regard to direct marketing
- **Rights in relation to automated decision-making and profiling**

15

15

Seven Principles of Data Protection

1. Data processing must be **lawful**, **fair** and **transparent**
2. For explicit legitimate **limited purposes** only
3. Hold no more data than necessary for the purpose (**data minimisation**)
4. Data must be kept **accurate** and up to date
5. Keep data for no longer than necessary (**storage limitation**), after which destroy, delete or return it
6. Keep data secure: protect against accidental loss, damage, disclosure (**integrity and confidentiality**)
7. Data controllers are **accountable** for compliance and must be able to demonstrate compliance

16

16

Six Lawful Bases for holding/processing data

1. **Legitimate interest** – needed for performance of main business, and 'balance of interests'
2. Necessary to fulfil **contractual obligation**
3. **Legal obligation** of the data controller
4. Data subject has given **consent**
5. Needed to protect **vital interests** (i.e. someone's life) of the data subject
6. **Public task**

For each type of data: decide which lawful basis is *most appropriate* for holding/processing that data. Get it right first time – there are implications!

17

17

Typical Parish Data: lawful bases (suggested)

Legitimate interest

- Parish office holders: PCC etc.
- Rota members (may be consent?)

Consent

- Membership
- Parish magazine / email (publicity)

Contractual obligation

- Employees

Legal obligation

- Pre wedding identity checks
- Electoral Roll
- Giving (Gift Aid)
- Registers (baptisms, marriages)

18

18

Other Requirements you should be aware of

Data storage
Data must be stored within the European Economic Area or, if stored outside, to standards equivalent to GDPR (e.g. Privacy Shield in USA)

Data sharing
Data controller's responsibility to control/restrict the use of data shared with other organisations (data sharing agreement).

Subject Access Request
- Request for copy of data held
- No charge, one calendar month to respond

Risk Management
- Encourage the reporting of **Data Breaches**: record and react
- Data Processing Impact Assessment (DPIA) for high risk activity (unlikely)

19

19

Registering with the ICO?

- Data controllers ***may*** need to register with the Information Commissioner's Office
- Many charities and not-for-profit organisations are exempt from registering … and therefore do not need to pay a fee.
- However … if you use CCTV for the purposes of crime prevention, registration is mandatory
- If you do have to register, and pay a fee, charities and not-for-profit organisations pay a Tier 1 fee of £40/year

Self assessment:
- ico register self assess
- ico how much will i need to pay

20

20

Useful Sources of Information

- Diocesan website: www.oxford.anglican.org/ (under Support Services, GDPR)
- ICO Guide to GDPR: ico.org.uk (under General Data Protection Regulation (GDPR))

21

GDPR: Journey to Compliance

22

22

Typical steps for parishes/deaneries:

DIOCESE OF OXFORD

1. Raise awareness
2. Conduct a Data Audit (and data mapping)
3. Identify (and document) your 'lawful bases'
4. Check your processes meet the 'eight rights' and 'seven principles'
5. Review how you get consent
6. Build in extra protection for children
7. Data retention and disposal
8. Review your Data Sharing
9. Update Policies & Privacy Notices
10. Work out how you will deal with Subject Access Requests
11. Data breaches: how will you detect, report and investigate?
12. Training
13. Build-in data protection to your new initiatives

rochester diocese gdpr toolkit
(simpler version at parishresources.org.uk/gdpr)

23

23

1. Raise awareness

DIOCESE OF OXFORD

- Discuss at PCC(s), standing committee, etc.
- Discuss the scope (e.g. for benefices)
- Identify your legal entities (incumbent, PCCs)

24

24

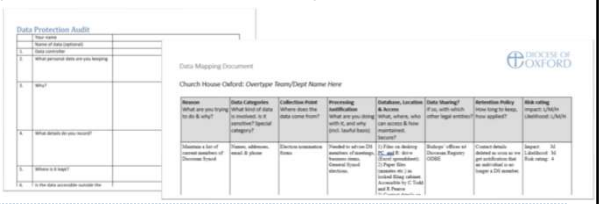
2. Conduct a Data Audit (and data mapping)

Data audit:

- list all the places where you handle personal data and what is that data

Data mapping (optional next step):

- helps you sort the different data into logical 'chunks'



25

25

3. Identify (and document) your 'lawful bases'

1. Legitimate interest
2. Contractual obligation
3. Legal obligation
4. Consent
5. Vital interests
6. Public task

Decide, in each case, which one is most appropriate.

26

26

4. Check processes meet 8 rights & 7 principles

1. Right to be informed (transparency)
2. Right of access
3. Right to rectification
4. Right to erasure
5. Right to restrict/suppress processing
6. Right to data portability
7. Right to object
8. Right in relation to automated decision-making and profiling

1. Processing: lawful, fair and transparent
2. For explicit and legitimate (limited) purposes only
3. Using the minimal data necessary
4. Kept accurate and up to date
5. Kept for no longer than necessary
6. Kept safe from corruption or unauthorised access
7. Data controllers: accountable and able to demonstrate compliance

27

27

5. Review how you get consent

- Decide when consent is needed (part of your 'lawful basis' decision)
- Giving consent:
  - Opt-in and Opt-out: equally straightforward
  - Cannot default to Opt-in
  - "Granularity": multiple Opt-ins must be separate, not linked
  - Must be freely given
  - Unambiguous
  - Use age-appropriate language
- Consent must be recorded for future reference
- Withdrawing consent – must also be recorded!

28

28

6. Build in extra protection for children

- Children's personal data merits specific protection (due to increased risks)
- Be clear about
  - where a child is the data subject
  - who gives consent for you to process data about a child?
- Any privacy notice or consent statement intended to be read by children must be in plain, age-appropriate, language
- Consult with children when designing processing of their data?
- Consent: no set age at which children are considered competent to provide their own consent to processing (under GDPR, 13 year-olds capable of giving consent for 'information society services')

29

29

7. Data retention and disposal

- How long do you need to keep the data?
  - When do you stop using it?
  - Do you need to archive it?
  - Records kept for safeguarding purposes?
- How you delete/dispose of it?
  - Deletion of electronic records
  - Regular (annual?) reviews of data e.g. of contacts in email/mobile phone

church of england records management
"Keep or Bin? The Care of Your Parish Records"

30

30

8. Review your Data Sharing

- Find out which legal entities you share data with
  - Who is the data controller and who is the processor?
- Examine the agreement you have with them from a data perspective
  - Does the agreement specify what data is shared and what the other party can and cannot do with the data
  - Look for commitments that they do not share the data further
- Ask them: are they GDPR compliant?
  - Beware of taking 'yes' for an answer – probe, check their website
  - Ask for a formal letter confirming that they comply (and will inform you if they cease to comply)
- Do you need further work: contract amendment, data sharing agreement?
- Prioritise the higher-risk organisations

31

31

9. Update Policies & Privacy Notices

- Sample privacy notice:
- church privacy notice for examples
  - Beware of copying other peoples' mistakes

32

32

10. Subject Access Requests

- Unlikely, but could be contentious if it happens
- At least have an outline plan of how you would handle a SAR

33

33

11. Data breaches

- Be aware of the possibility of a data breach
- Likely risk areas:
  - Loss/theft of data (e.g. laptop, phone or tablet stolen)
  - Email or social media account hacked
  - CVs or other sensitive/confidential documents disclosed
- How will you detect, report and investigate?

34

34

12. Training

- What additional awareness or skills might be required?

35

35

13. Build-in data protection to your new initiatives

- 'Privacy by design': you make data protection considerations when introducing new activities and areas of involvement
- Risk assess new activity (DPIAs) watch out for:
  - Linked databases
  - Vulnerable data subjects (elderly, children, those who are unwell)
  - New technologies

36

36