

# GDPR FOR CHURCHES

Ashford Archdeaconry  
12 April 2018

---

---

---

---

---

---

---

---

CHANGED LIVES @ CHANGING LIVES

## WHAT IS GDPR?

“GDPR rebalances the relationship between individuals and organisations. It gives greater control to people about how their data is used and it compels organisations to be transparent and account for their actions.”

*Elizabeth Denham, Information Commissioner*



---

---

---

---

---

---

---

---

CHANGED LIVES @ CHANGING LIVES

## WHAT ABOUT BREXIT?



---

---

---

---

---

---

---

---

# KEY TERMS

- **Personal data:** information about a living individual which is capable of identifying that individual. Data subject
- **Data subject:** person about whom personal data is processed
- **Data controller:** person/organisation who determines the how and what of data processing
- **Data processor:** responsible for processing personal data on behalf of a controller
- **Processing:** anything done with/to personal data, including storing it




---

---

---

---

---

---

---

---

---

---

# KEY PRINCIPLES

Personal data must:

- be processed **lawfully, fairly and transparently**
- only used for a **specific processing purpose** that the data subject is aware of - and no other without further consent
- be "**adequate, relevant and limited**"
- be "**accurate** and where necessary **kept up to date**"
- not be stored for **longer than is necessary**
- be processed in a manner that ensures appropriate **security and protection**




---

---

---

---

---

---

---

---

---

---

# WHAT'S NEW?

- Consent: **informed, opt-in**
- New **rights** for data subjects
- Data should only be used for **purpose it was gathered for & deleted** when no longer required
- **Tougher sanctions** for non-compliance & for sharing data outside the EEA
- Staff & data users should have suitable **training & advice**
- Serious **data breaches** must be reported to ICO within 72 hrs
- Principle of **accountability** – onus on data controller




---

---

---

---

---

---

---

---

---

---

## RIGHTS OF THE DATA SUBJECT

1. The right to be **informed**
2. The right of **access**
3. The right to **rectification**
4. The right to **erasure**
5. The right to **restrict processing**
6. The right to **data portability**
7. The right to **object**
8. Rights in relation to **automated decision making and profiling.**




---

---

---

---

---

---

---

---

---

---

## DON'T PANIC




---

---

---

---

---

---

---

---

---

---

## LEGAL BASIS FOR HOLDING DATA

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




---

---

---

---

---

---

---

---

---

---

# SPECIAL CATEGORY DATA

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics
- health
- sex life
- sexual orientation




---

---

---

---

---

---

---

---

# PROCESSING SPECIAL CATEGORY DATA

1. Explicit consent
2. Employment law
3. Vital interests
4. Charities, religious organisations, and not-for-profit
5. Made public by data subject
6. Legal claims
7. Public interest
8. Medical diagnosis/treatment
9. Public health
10. Historical, statistical or scientific purposes




---

---

---

---

---

---

---

---

# CONSENT

“...any freely-given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”




---

---

---

---

---

---

---

---



CHANGED LIVES @ CHANGING LIVES

# LEGITIMATE INTEREST

- Most flexible – but more responsibility
- 3 part test:
  1. Identify a legitimate interest
  2. Show that the processing is necessary to achieve it
  3. Balance it against the individual's interests, rights and freedoms.
- Document it




---

---

---

---

---

---

---

---

---

---

CHANGED LIVES @ CHANGING LIVES

# BREATHE




---

---

---

---

---

---

---

---

---

---

CHANGED LIVES @ CHANGING LIVES

# GIFT AID

- Consent needed on declarations
- Oct '17 – 12,655 declarations but only 5,300 active
- To date have received approx 4,400
- As at 25 May, **all non-GDPR declarations will expire**




---

---

---

---

---

---

---

---

---

---

CHANGED LIVES ⇄ CHANGING LIVES

## GIFT AID

- One-off declarations (pew envelopes) also need to have consent built in
- We can provide stickers for existing stocks
- If re-ordering, ensure wording is compliant




---

---

---

---

---

---

---

---

CHANGED LIVES ⇄ CHANGING LIVES

## GIFT AID

- Legitimate Interest for gift aid secretaries / treasurers
- All data to be retained for seven years\*




---

---

---

---

---

---

---

---

CHANGED LIVES ⇄ CHANGING LIVES

## CONTACT LISTS

- Consent or Legitimate Interest?
- Be clear
- Make sure people know their rights




---

---

---

---

---

---

---

---

# CHILDREN

- If you process children’s data, their protection is paramount
- Compliance with the data protection principles should be central
- Lawful basis required
- 13 is age of consent – otherwise, guardians must give consent
- Make your privacy notices clear so that children are able to understand their rights & what will happen to their data
- Children have the same rights as adults




---

---

---

---

---

---

---

---

# THIRD PARTIES

- Charities
- Partners
- Diocesan staff
- Bishop’s office
- Archdeacon’s office
- Online service providers – Eventbrite, Mailchimp, JustGiving WordPress...




---

---

---

---

---

---

---

---

# ELECTORAL ROLL

- Data protection rules apply unless there is a specific legal requirement to do otherwise
- The Synodical Government Measure requires that the **names** of those on the electoral roll be displayed and therefore that takes precedence over data protection regulations




---

---

---

---

---

---

---

---



## DATA BREACHES

“the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.”

---

---

---

---

---

---

---

---



## DATA BREACHES

1. Establish the likelihood & severity of the risk to people’s rights and freedoms
2. If it’s likely that there will be a risk then you must notify the ICO **within 72 hrs**. Where it’s serious, notify data subject **immediately**
3. If it’s unlikely, don’t report but document & be willing to justify your decision

---

---

---

---

---

---

---

---



## ACCESS REQUESTS

- Individuals have right to obtain:
  - confirmation that their data is being processed
  - access to their personal data
  - other info related to privacy and use of their data
- Free of charge - unless excessive
- Respond within one month - unless complex

---

---

---

---

---

---

---

---



### DATA PROTECTION IMPACT ASSESSMENT

- Identify & minimise data protection risks of a project
- Applicable for certain listed types of processing, high risk processing or a major project which requires the processing of personal data
- A DPIA must:
  - describe the nature, scope, context and purposes of the processing;
  - assess necessity, proportionality and compliance measures;
  - identify and assess risks to individuals; and
  - identify any additional measures to mitigate those risks.
- If you identify a high risk and you cannot mitigate that risk, you must consult the ICO before starting the processing.




---

---

---

---

---

---

---

---

---

---

### DATA PROTECTION OFFICER

- Not required for parishes under GDPR, but good practice to have a named person responsible for data
- Diocesan DPO – Anna Drew (07753454586 / adrew@diocant.org)




---

---

---

---

---

---

---

---

---

---

### IT'S GOING TO BE OKAY




---

---

---

---

---

---

---

---

---

---

# WHAT TO DO NOW

1. **Audit:** what data do you hold? How secure is it? Who do you share it with? What consent do you have?
2. **Update** systems, forms & policies
3. **Train**/advise those who handle data
4. **Check** that data processors are GDPR compliant
5. **Document** everything

---

---

---

---

---

---

---

---

# CONSIDER:

1. Is what I'm doing in accordance with the Data Protection principles?
2. Am I upholding the terms of our Privacy Notice?
3. If someone made a subject access request, is there anything I'd wish I'd done differently or would find hard to justify?

---

---

---

---

---

---

---

---

# RESOURCES

- GDPR Checklist GDPR & Safeguarding: advice from the Nation Church
- Parish Data Audit Form
- Care of Parish Records
- Parish Consent Form Template
- Parish Privacy Notice Template (non-role holders)
- Parish Privacy Notice Template (role holders)
- DPIA Checklist
- Template Baptism Contact Form

---

---

---

---

---

---

---

---

## USEFUL LINKS

- [WWW.CANTERBURYDIOCESE.ORG/GDPR](http://WWW.CANTERBURYDIOCESE.ORG/GDPR)
- [WWW.GDPRFORCHURCHES.ORG.UK](http://WWW.GDPRFORCHURCHES.ORG.UK)
- [WWW.PARISHRESOURCES.ORG.UK/GDPR](http://WWW.PARISHRESOURCES.ORG.UK/GDPR)
- [WWW.CHURCHOFENGLAND.ORG/MORE/LIBRARIES-AND-ARCHIVES/RECORDS-MANAGEMENT-GUIDES](http://WWW.CHURCHOFENGLAND.ORG/MORE/LIBRARIES-AND-ARCHIVES/RECORDS-MANAGEMENT-GUIDES)
- [WWW.ICO.ORG.UK/FOR-ORGANISATIONS/GUIDE-TO-THE-GENERAL-DATA-PROTECTION-REGULATION-GDPR/](http://WWW.ICO.ORG.UK/FOR-ORGANISATIONS/GUIDE-TO-THE-GENERAL-DATA-PROTECTION-REGULATION-GDPR/)




---

---

---

---

---

---

---

---

## QUESTIONS?




---

---

---

---

---

---

---

---