General Data Protection Regulation

Rebekah Fozzard
Manager – Special Projects and GDPR Coordinator
Representative Church Body
July 2018

Recap:
General Data Protection Regulation

European data protection regulation

Overhauls and harmonises existing data protection law

New responsibilities on organisations

Non Compliance can lead to **Large Fines**!

Came into Effect

Common terms

Data Subject – natural living person

Data Controller – how and what

Personal Data - identifiable information

Processing Data – how you use it

Special Category Data - sensitive

GDPR principles that need to be adhered to

- Fairly obtained
- Processed lawfully, fairly and transparently
- Only used for the specific purpose you received permission for, and no other purpose
- Is adequate, relevant and limited
- Is accurate and kept up to date
- Is only stored for as long as is necessary
- Is kept safe and secure

Individual rights

BE INFORMED

ACCESS their personal information

Have personal data ERASED

Have personal data CORRECTED

RESTRICT processing

OBJECT

Data PORTABILITY

No AUTOMATED decision making

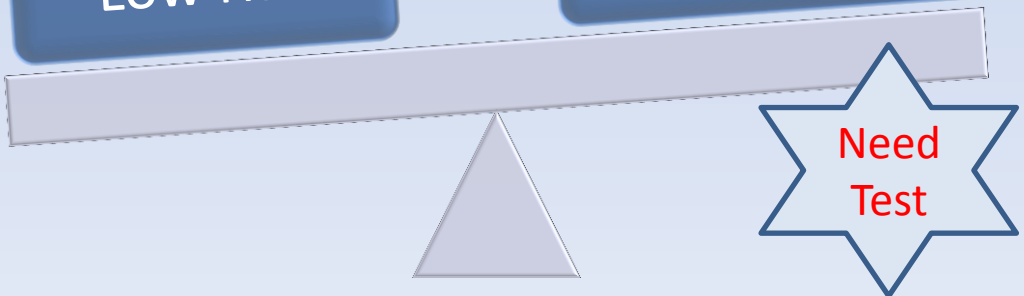
Ways to process personal data

Consent

- Freely given
- Specific
- Informed
- Affirmative action
- Written or verbal
- Can be **WITHDRAWN**

Legitimate Interest

Data Controller	Data Subject
Necessary	Fundamental Rights
Reasonable expectations	Freedoms
Safeguards	Interests
Low risk	



Other ways to process personal data

- **Contractual Necessity**

Needed to enter into or perform a contract

- **Public Interest**

e.g. CCTV for safety reasons

- **Compliance with Legal Obligation**

e.g. Revenue Reporting

- **Vital Interest**

Life or death

Managing a Data Breach

What is a breach?

- accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data

What do you do?

- Follow your procedure and:
  - document the facts relating to the breach, its effects and the remedial action taken
  - keep a log of breaches, large and small
  - if the breach is likely to result in a high risk to individuals you must let them know asap
  - if a serious breach, contact the Data Protection Commissioner no later than 72 hours after becoming aware of the breach

GDPR and Photography

- Where a photograph can clearly identify an individual, consent should be sought, particularly if this photograph will be published on any external site (e.g. website).
- Photographs should be treated the same as any other personal data
- Where photographs of minors/children e.g. under 16 years old are used, then guardian consent must be obtained – this is mandatory
- Where a photograph can not uniquely identify a person, so a data subject is not at risk should the data be comprised, it is possible to use this photograph within the legitimate interests of the work of the Parish

Subject Access Request

- ❑ Individuals have the right to access their personal data
- ❑ Individuals can make a subject access request verbally or in writing
- ❑ You have one month to respond to a request
- ❑ You cannot charge a fee unless excessive
- ❑ You can refuse if repetitive or vexatious

Top Tips!

- Develop a form for individual to complete
- Check their ID
- Communicate and keep in touch with the requester
- Watch out for personal data pertaining to others – it cant be shared without consent

What each Parish needs to do

Awareness

- Agree who is in charge
- Data Controller = Parish
- Develop internal data security policy e.g. passwords; Pins; Locked cupboards
- Set up GDPR file

Know your Information

- Review all personal data held
- Identify & implement actions (e.g. seek consent, archive/delete)
- Identify legal basis for processing
- Develop procedure to manage consent
- Do legitimate interest test if required

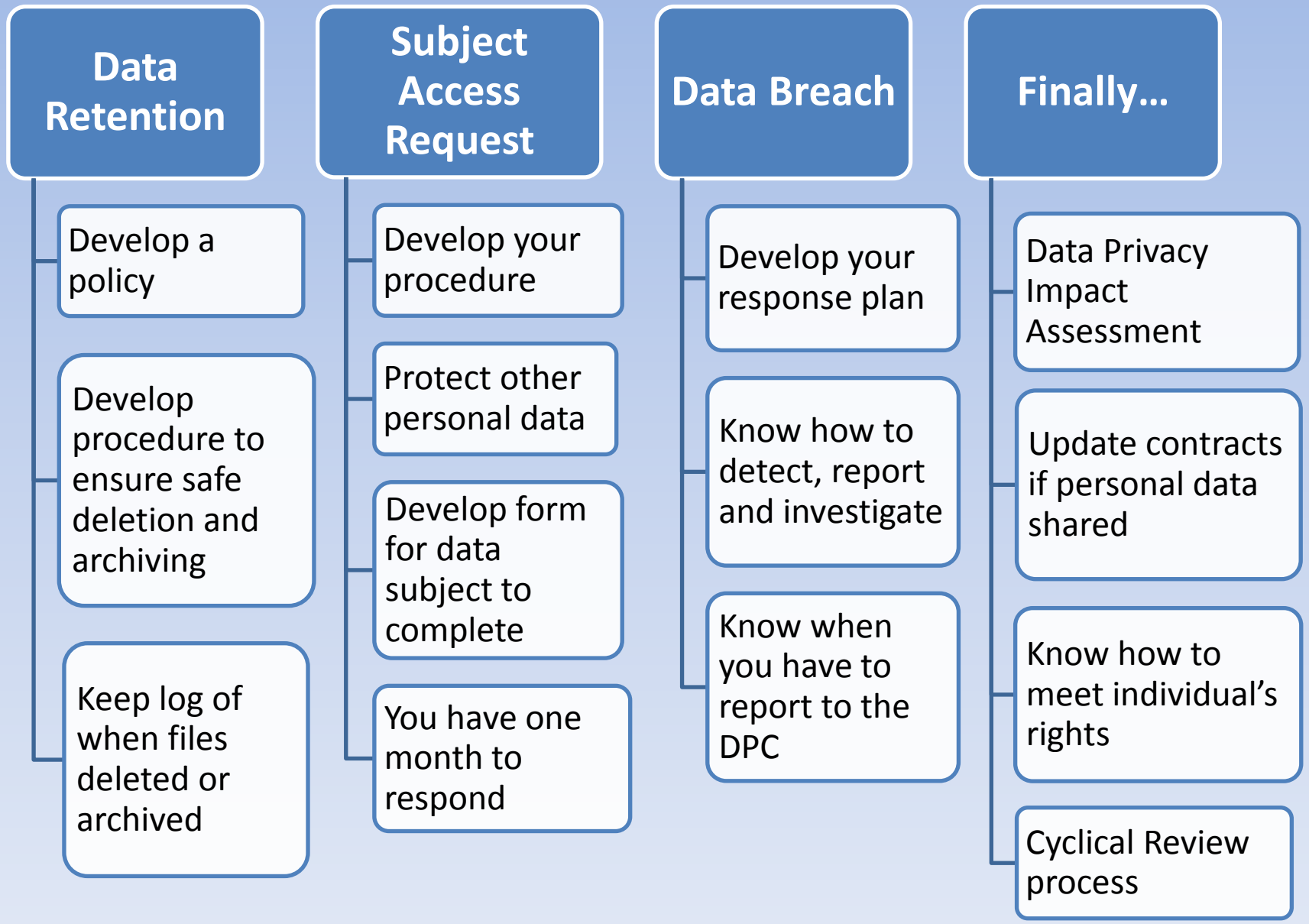
Special Category Data

- Develop a policy
- Divide into categories e.g. children
- Identify a legal basis for processing each type of SCD
- Include that 'you are processing SCD within the legitimate activities of the COI'

Communicate

- Website Data Privacy Notice
- Parish Data Privacy Policy (internal)
- Reoccurring agenda item at SV meetings
- Poster on noticeboard

What each Parish needs to do



Questions?

Best of Luck

*The road to success is not straight. There is a curve called **Failure**, a loop called **Confusion**, speedbumps called **Friends**, red lights called **Enemies**, caution lights called **Family**. But, if you have a spare called **Determination**, an engine called **Perseverance**, insurance called **Faith**, a driver called **Jesus**, you will make it to a place called **Success.***

Appendix
Legitimate Interest: at a glance!

Legitimate interest is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact

If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.

There are three elements to the legitimate interests test. You need to:

identify a legitimate interest;
show that the processing is necessary to achieve it; and
balance it against the individual's interests, rights and freedoms

- The legitimate interests can be your own interests or the interests of third parties.
- They can include commercial interests, individual interests or broader societal benefits.
- The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.
- You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.

Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required.