Data Protection and the GDPR

(General Data Protection Regulation)

24 May 2018 – Second Presbyterian Church Comber

1. Background to GDPR

Why do we need GDPR?

- EU Directive drafted prior to internet age – not "fit for purpose"
- Personal data is now used in ways that didn't exist in 90s
- The types of personal data collected and held have also changed – biometric data, genetic data, images
- This new legislation, GDPR, aimed at giving us, as individuals, more information and control over our personal data - comes into effect from 25 May

2. Essential terminology

Personal Data

… any information relating to an identifiable natural person. That is an individual who can be identified directly or indirectly in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

2. Essential terminology

Examples of personal data include?

- Name
- Address
- Postcode
- Phone number
- email address
- National Insurance number
- Photograph
- ip address, etc.

2. Essential terminology

Under GDPR there are special categories of personal data;

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trades Union membership
- Physical or mental health or condition
- Sexual life or sexual orientation
- Genetic data
- Biometric data

2. Essential terminology

Data Subject

… a natural person whose personal data is processed by a Data Controller This **does not include a deceased person** or somebody who cannot be identified or distinguished from others.

2. Essential terminology

In a Congregation the data subjects will include:

- Members
- Individuals receiving pastoral care
- Children/young people attending BB, GB, Holiday Bible Clubs, Sunday School, Youth Groups, Crèche
- Gift Aid donors
- Contacts via a web site
- External users of our premises
- Suppliers, tradesmen
- Staff etc.

2. Essential terminology

Data Controller

… a body which determines the purposes and means of the processing of personal data.

(for the congregation the Kirk Session will be controller)

2. Essential terminology

Acting for the data controller

- Minister
- Elders
- Organisational leaders
- Gift Aid secretary
- Treasurer
- Volunteers
- etc.

2. Essential terminology

Data Processor

This essentially means a ***third party*** e.g.

- IT provider (e.g. cloud storage)
- Payroll provider

2. Essential terminology

- **GDPR requires a Processor to:**
  - Act only on documented instruction and use the personal data for agreed purposes.
  - Persons authorised to access under obligation of confidentiality.
  - Assist with Data Subject Rights, Data breaches
  - Return or delete Personal Data when service ends.
  - Demonstrate compliance

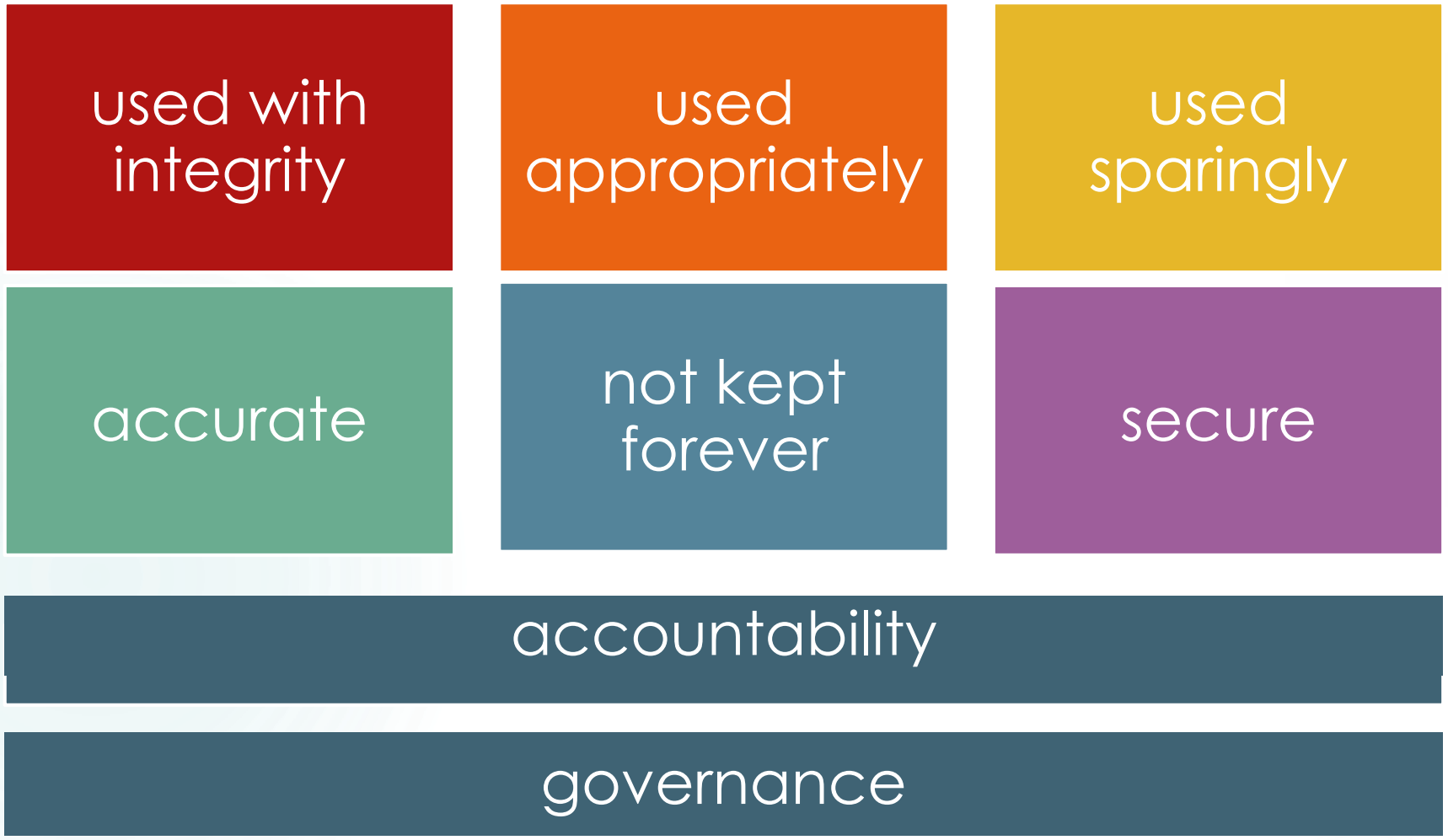
2. Essential terminology

Processing

… any operation or set of operations performed on personal data or sets of personal data whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

…basically it is anything at all you do with the data

3. Principles under GDPR (Article 5)



3. Principles under GDPR (Article 5)

The Lawfulness and Transparency Principle

used with integrity

processed **lawfully, fairly and in a transparent manner** in relation to individuals

[To be used lawfully you must be able to rely on at least one of six legal bases for processing i.e. there must be a legitimate reason for us processing someone's personal data]

3. Principles under GDPR (Article 5)

The Purpose Limitation Principle

Used appropriately

Collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those stated purposes; *further processing for archiving purposes in the public interest or for scientific, historical research or statistical purposes shall not be considered incompatible with the initial purpose.*

[Need to be clear about reason for collecting personal information and ensure it is only used for that purpose]

3. Principles under GDPR (Article 5)

The Data Minimisation Principle

used sparingly

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

[Don't hold it if you can't demonstrate a need]

[Only collect what information you need e.g. if you don't need someone's work phone number don't collect it]

3. Principles under GDPR (Article 5)

The Accuracy Principle

accurate

accurate and, where necessary, kept up to date; every reasonable effort must be taken to ensure that personal data that is inaccurate having regard to the purposes for which is processed is erased or rectified without delay;

[Otherwise confidential information could, for example, go to the wrong address]

3. Principles under GDPR (Article 5)

The Storage Limitation Principle

not kept forever

kept in a form which permits identification of data subjects **for no longer than is necessary** for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as it will be processed solely for archiving purposes in the public interest, or for scientific, historical research or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

[Clear out redundant personal data – data we no longer need or use for its original purpose]

3. Principles under GDPR (Article 5)

The Integrity and Confidentiality Principle

secure

processed in a manner that ensures **appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Principles under GDPR (Article 5)

The Integrity and Confidentiality Principle3.

secure

For example

- Passwords should be kept secure, should be strong, changed regularly
- Use bcc when emailing to a large number of people
- Confidential waste – shredded
- Preventative measure re virus attacks
- Keep back-ups
- Encrypt data taken off PCs / laptops
- Hard-copy material kept secure

3. Principles under GDPR (Article 5)

accountability

- The controller must be able **to show that they are complying with these principles**
- Requirement to have documentary evidence of consent, data processed and legal basis for processing
- Burden of proof on data controller to demonstrate compliance with principles of GDPR

3. Principles under GDPR (Article 5)

accountability

- Data audit
- Data Protection Policies
- Staff Training
- Internal review
- Maintain record of processing activities
- Data Protection Officer (or Lead)
- Data minimisation, pseudonymisation, transparency

3. Principles under GDPR (Article 5)

governance

The practical measures you put in place, **the steps that you have taken so that you can demonstrate compliance under the principles above – these then are the means by which you have implemented good governance**. This can be achieved by documenting the decisions you take about processing personal data, undertaking training, reviewing policies and procedures such as data protection, privacy notices, consent etc.

4. Legal basis for processing

- Having a lawful basis for each processing activity is critical to an organisation's ability to comply with GDPR
- Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law.
- If the Controller does not have a lawful basis for a given data processing activity then that activity is essentially unlawful.

4. Legal basis for processing

Legal basis available (six):

- Consent of the data subject *(Article 6(1)(a))*
- Necessary for performance of a contract *(Article 6(1)(b))*
- Compliance with a legal obligation *(Article 6(1)(c))*
- Protect the vital Interests of a data subject *(Article 6(1)(d))*
- Task carried out in the Public Interest *(Article 6(1)(e))*
- Legitimate interests pursued by the controller *(Article 6(1)(f))*

(then there are Special Categories of Data which can inform legal basis – examples later)

4. Legal basis for processing

Mostly we will rely on

- Legitimate interests
- Only rely on consent as a last resort

If someone withdraws consent you will have difficulty processing the data in question

4. Legal basis for processing

Legitimate interests

- Can be that of the congregation or presbytery
- Or the legitimate interest of a third party

That an individual has a reasonable expectation that you will process their data for a particular purpose makes it likely that processing on this basis will be lawful

4. Legal basis for processing

Consent - use as basis of "last resort"

Under GDPR must be;

- Freely given, specific, informed and an unambiguous indication of the individual's wishes
- There must be some form of clear affirmative action i.e. a positive opt in
- Must be capable of being withdrawn
- Has to be verifiable
- Must be separate from other written matters

4. Legal basis for processing

Special Categories – there are 10 subsidiary legal bases for processing Special Categories of data identified in the legislation. Most relevant ones include:

- Obligations under employment *(Article 9(2)(b))*
- Vital Interests – subject cannot give consent *(Article 9(2)(c))*
- Not for Profit body, no 3rd party disclosure *(Article 9(2)(d))*
- Archiving Data in the Public Interest *(Article 9(2)(j))*

4. Legal basis for processing

Article 9(2)(d))

Processing carried out by a not for profit body with a political, philosophical, **religious** or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is **no disclosure to a third party** without consent.

5. Data Subject Rights

1. The right to be informed (Privacy Notice)
2. The right of access (Subject Access Request)
3. The right to rectification
4. The right to erasure (right to be forgotten)
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

Summary

- Don't panic : prepare
- Requirement to comply
- Follow the six key principles - used with integrity, used appropriately, used sparingly, kept accurate, not kept for ever, kept secure, AND underpinned with accountability and governance.
- Consider your processing activities and the appropriate lawful basis for processing
- Remember data subject rights, consequences of breaches
- Penalties

……. so how do we achieve compliance and how can PCI help?

4. Legal basis for processing

Processing Activity	Lawful Basis	Special Data
Membership list	Legitimate	Not for profit
Coffee Rota	Legitimate	N/A
Church weekend	Legitimate	Not for profit
Staff	Contract & Legal	Employment
Pastoral records	Legitimate	Not for profit
Prayer chain	Legitimate	N/A
Youth Club (<13)	Consent (Parental)	Not for profit
Youth Club (13-16)	Consent (Both)	Not for profit

Legal basis for processing

Processing Activity	Lawful Basis	Special Data
Letting of premises	Contract	N/A
Gift Aid donors	Legal	Not for profit
Parent emergency contact	Vital interests	Vital interests
Home Groups	Legitimate	Not for profit
Special Need Club	Vital Interests	Vital Interests
Herald subscribers	Consent	Not profit
…….		

Data Breaches

Most likely source of concern!

Most likely causes of breach:

- Weak or stolen credentials (log-in + password)
- Back Doors, Application Vulnerabilities
- Malware
- Accidental loss
- Physical Theft
- Hack attack