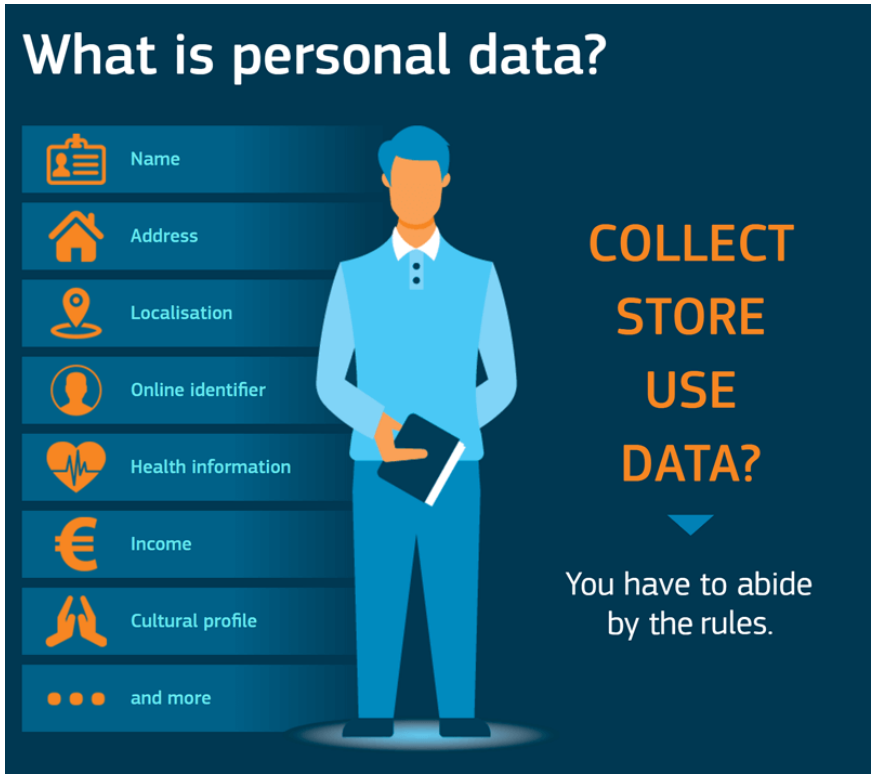
Stirling Presbytery
Chris Wilson
www.dunblanecathedral.org.uk

Quick Reminder



- Data Protection refers to “personal data” of living individuals – not businesses, or organisations, or other data, or if you’re dead!
- Personal Data is
  - data which relates to a living individual who can be identified –
    - (a) from that data, or
    - (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller (Stirling Presbytery and its churches), i.e. **IMPLIED**
  - and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

What is GDPR?

- **GENERAL DATA PROTECTION REGULATION** (GDPR) becomes law in all EU states on 25th May 2018
  - Replaces the current Data Protection Laws
- There are big changes which have an impact on organisations, businesses and charities
  - Elders/trustees of our churches, must be aware of these changes and how they affect us

Who benefits from GDPR?

- Every individual should welcome GDPR:
  - You are the OWNER of your personal data – name, address, email, phone number, etc. Anything which can identify you.
  - Only YOU can decide who has the right and need to hold your data
  - You have the RIGHT to be guaranteed that your data is being held securely and managed properly
  - You have the RIGHT to know that your data is only being accessed by those with a valid authority and right to do so
  - It places CONTROL of your personal data back in your hands
  - It allows you to give or remove PERMISSION for your data to be held
  - You have the RIGHT to request to view, change, or delete the data held
- We, as **STEWARDS** of their data must be able to meet those demands

What about Brexit?

- We are still members of the EU – we must comply with all their laws until such times we leave on 29 March 2019
- 21 June 2017 - the UK Government confirmed its intention to bring the EU GDPR into UK law post Brexit
  - Data Protection Bill coming law immediately we leave - 2019
- If we share data with any part of the EU, we must comply with their data laws.
- Politically, no party will even consider making UK citizens less safe than their EU equivalents!

GDPR – the reality

- It's the law
  - The ultimate fine for non-compliance by your church is **€20,000,000**.
  - We should be complying, not because of the fine, but because morally and legally we should be doing the "right thing"
- It's our insurance
  - It's not all "cut and dried" – some of this will be left to the courts to decide
  - We must be able to show "best endeavours"
  - We must protect our Church, our Presbytery and our Trustees/Elders
- Like ignoring servicing a car, we will only feel the pain when it all goes wrong!

V

GDPR – The Details I

- **1. Personal data - enhanced**
  - The GDPR will **enhance** the definition of personal data as it will now also include identification numbers, location data and online identifiers to reflect technological advances in society.
- **2. Sensitive personal data - enhanced**
  - The GDPR will now include genetic and biometric data and will **omit criminal convictions and offences** from its definition of sensitive personal data.
- **3. Subject Access Requests – changed**
  - The rules around Subject Access Requests (SARs) will change in the GDPR. The GDPR will **remove the fee** that is chargeable under the DPA and will reduce the time limit during which an organisation must respond to a request to **1 month**, down from the 40 days currently available under the DPA.

GDPR – The Details II

- **4. Right to data portability – new**
  - The right to data portability will be a completely new right under the GDPR, allowing individuals to receive their personal data in an organised, **machine-readable** format.
- **5. Right to erasure – changed**
  - The GDPR will explicitly outline the **right to erasure** and will no longer require individuals to prove that the processing of their personal data caused them substantial damage or distress, which is currently a requirement under the DPA.
- **6. Record-keeping requirements – new**
  - The GDPR will place a new obligation on organisations to maintain **internal records** of all data processing activities.
- **7. Accountability principle – new**
  - The GDPR will introduce a new '**accountability principle**' in an effort to increase accountability and effective governance in data processing. (**Demonstrate** you comply)

GDPR – The Details III

- **8. Data protection by design and by default – new**
  - The GDPR will encourage a 'privacy by design' approach to data protection known as **data protection by design and by default**. This will require organisations to adopt measures that adhere to GDPR data protection principles such as data minimisation and pseudonymisation.
- **9. Data protection officer (DPO) – new**
  - The GDPR will create a new obligation for some organisations to appoint a **Data Protection Officer** who will be responsible for ensuring the organisation's compliance with the GDPR.
- **10. Penalties – enhanced**
  - The GDPR will levy **higher fines** than the DPA. Monetary fines will increase to €20 million or 4% of the annual global turnover of the previous financial year (whichever is higher).

GDPR – the Principles

GDPR states, in the following 6 principles, that personal data be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
6. processed in a manner that ensures appropriate security of the personal data.

We, as our Churches, must "be responsible for, and be able to demonstrate, compliance with the principles."

GDPR for Charities I

- There is no significant charity exemption to data protection or marketing law. Maybe there should be. There isn't.
- The ends never legalise the means.
- If a donor or other individual does not understand what you are doing with their personal data, the practical effect is that you can't do it, whatever it is. The same is true for consent – if a person doesn't understand what you're doing, you can't argue that they have consented to it.

GDPR for Charities II

- You don’t need consent for every use of personal data, but if you don’t have consent, you need to know what other justification you have that allows you to use the data. The other reasons are specifically set out in the Data Protection Act and the GDPR.
- You cannot assume consent. Failure to opt-out is not consent. Silence is not consent. Previous support is not consent. A donation I give you today is not consent for something tomorrow.
- Volunteers are no different to employees; they must be trained and equipped to protect data. There is no volunteer exemption. Using volunteers is a choice you have made, and you are responsible for ensuring that you manage the risks adequately.

GDPR for Charities III

- If you contract out any work to an agency or contractor, you are wholly responsible for what they do, unless they steal your personal data or otherwise use it for their own purposes.
- Personal data available in the public domain is still personal data and Data Protection still applies to it.
- There are specific rules for consent over the method of communicating fundraising and other direct marketing communications. Beyond that, you have to decide whether you need consent or whether some other condition applies

"Proportionality….. something that data protection legislation is lacking in my opinion."

What does this apply to in churches?

- Staff/payroll records
- Membership lists
- Cradle Roll
- Membership roll
- Baptismal records
- Gift Aid donations
- Names on the website e.g. rotas
- Information for Pastoral Care
- Holiday clubs or activities
- Sunday schools, youth groups, crèches
- Contact lists
- Digital photographs & videos where individuals can be identified

ALL Church data is “special category data” i.e. sensitive as it “reveals a person’s…religious or philosophical beliefs”

Legitimate Interest and Archival

- MOST data will be covered by “legitimate interest/activities” or “archival”
  - “Legitimate interest/activities” is generally how we can hold the data
  - “Archival” is how we can continue to hold data when the individual moves away
- “Legitimate Interest” means:
  - Consent has been given – not the best option, as it can also be withdrawn, and getting it can be fraught with issues ✗
  - Processing is necessary as part of a contract e.g. staff/payroll records ✓
  - Necessary for the purposes of the legitimate interests of the church ✓
    - Cannot override the rights & freedoms of the individual especially if a child
    - This is the preferred option, HOWEVER we must
      - Identify a legitimate interest
      - Establish that the processing is necessary
      - Test that our interests are “balanced” with those of the individual

What are the tasks of the DPO?

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.)

What does the GDPR say about DPO reporting?

- You must ensure that:
- The DPO reports to the highest management level of your organisation – i.e. Kirk Session.
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Adequate resources are provided to enable DPOs to meet their GDPR obligations.
- You can also contract out the role of DPO externally.

Does the DPO need specific qualifications?

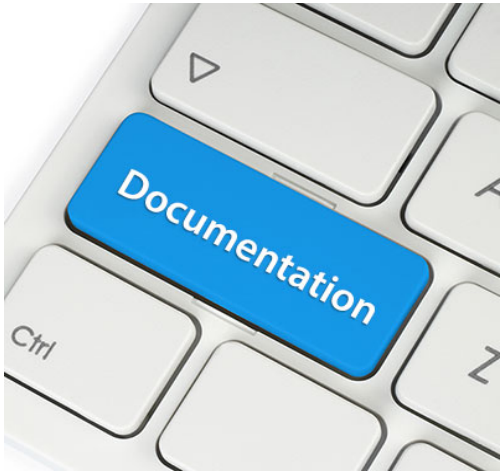
- The GDPR does not specify the precise credentials a data protection officer is expected to have.
- It does require that they should have professional experience and knowledge of data protection law. This should be proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the personal data requires.

Report Categories

- Special category data = sensitive data e.g.
  - race;
  - ethnic origin;
  - politics;
  - religion;
  - trade union membership;
  - genetics;
  - biometrics (where used for ID purposes);
  - health;
  - sex life; or
  - sexual orientation.
- Identify individuals' categories e.g. members, adherents, attendees, employees

Documentation – what do I need?*

- The name and contact details of your organisation and your Data Protection Officer.
- The purposes of your processing.
- A description of the categories of individuals and personal data.
- The categories of recipients of personal data.
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of your technical and organisational security measures.
- Information required for privacy notices, such as:
  - the lawful basis for the processing
  - the legitimate interests for the processing
  - individuals' rights
  - the existence of automated decision-making, including profiling
  - the source of the personal data;
- records of consent ;
- the location of personal data;
- your retention and erasure policy document.



What actions do we need to take? I

- Appoint a Data Protection Officer for your church
  - Use this network for questions and advice
  - Ask another local church to share their DPO?
- Perform a data audit
  - What data does your church and its organisations hold?
  - What data do you share with other organisations e.g. BB, GB, RVS?
  - Have you permission to share the data?
  - How accurate is the data?
  - How are you keeping it current?
  - A LIA (Legitimate Interests Assessment) form is due from Law Department
- Balancing Test
  - Balance your interests against the individual's
    - Reasonable expectation and no harm

What actions do we need to take? II

- *Do NOT use non-GDPR complaint emails on Church business
  - Ministers should be using the Church of Scotland email system
  - Churches should sign up for the Microsoft Office 365 E1 product for NPOs – free
  - Create emails for the roles within your church who require email
    - Treasurer, Safeguarding, DPO, Session Clerk, etc
- Data must be current and accurate
  - Schedule regular verification of data, even informally
- Document your GDPR processes as required for Church of Scotland*

Remember…

- Anything which contains personal comments or data referring to individuals is subject to GDPR – this includes emails
  - The data must therefore be searchable, editable and able to be deleted
  - If it could be used as evidence in law to show what an action was taken, then it needs to be kept
- It can be extremely difficult to extract personal data from non-personal data.
  - Often it is simpler to take a single approach to all data
- Two terms to use: "**legitimate interests with APPROPRIATE SAFEGUARDS**" and "**archival**"
  - We MUST NOT pass data to another organisation without express consent
- We may have permission to hold the data, but we must do our best to keep it current and accurate
- Get rid of data you don't need
- With GDPR – YOU ARE NOT ALONE!

GDPR

www.dunblanecathedral.org.uk
Look for Presbytery at the bottom of the screen
Password is **Stirling-presbytery-Files**

chrisstirlingpres@btinternet.com

Stirling Presbytery DP Network

07545 427377

Stirling Presbytery
Chris Wilson
www.dunblanecathedral.org.uk