Data Protection and GDPR for Parishes

Andrew Gallie

vwv.co.uk | Offices in London, Watford, Bristol & Birmingham
Lawyers & Parliamentary Agents

Part 1: Data protection essentials

What is data protection and personal data?

Data protection:

- regulates the use of personal data; and
- gives people rights in their personal data.

Personal data is information:

- from which an individual can be identified (directly or indirectly)
- which relates to that individual
- not just factual - opinions count

Special and confidential personal data

Why is data protection important?

- Fines increasing from the current £500,000 to the higher of €20 million or 4% of annual worldwide turnover
- Compensation payments to affected individuals
- Bad publicity and reputational damage – media interest
- Staff and clergy can be personally liable if they use personal data for their own purposes. This includes anyone who holds the Bishop's licence to exercise ministry in the Parish
- Complaints
- Data protection vs safeguarding and child protection
- Regulated by the Information Commissioner's Office (ICO)

Data Protection Principles

GDPR requires that personal data be:

1. Processed lawfully, fairly and in a transparent manner.
2. Collected for specified legitimate purposes and not further processed in a manner which is incompatible with those purposes.
3. Adequate, relevant and not excessive
4. Accurate and kept up to date
5. Not kept for longer than is necessary for the purposes for which it was obtained.
6. Processed in a manner that ensures appropriate security e.g. not accidently lost, damaged etc.

Question

From what age can children exercise their rights under data protection law?

1. There is no minimum age
2. Twelve
3. Sixteen
4. Eighteen

Children

- Children can exercise their own data protection rights when they are sufficiently mature.
- In many cases, it is reasonable to assume that a child will have the necessary maturity from and including the age of 12 years old.
- Parents will exercise their child's data protection rights on their behalf until their child is sufficiently mature.
- Sometimes sharing information with a parent can be a breach of the child's data protection rights
- How does the GDPR change matters?

Step 1: Where to begin with GDPR preparations

GDPR:
What should you be doing now?

- Audit your data flows, e.g, categories of data, sources and recipients
- Keep a record of what you are doing to become GDPR compliant. For example, do we need a DPO?
- Information and asset registers
- Guidance and templates, eg, Parish Resources and the ICO

Step 1: Record keeping

Accountability

- Must “demonstrate” compliance. For example, documenting consents, legitimate interests assessment, and special category data policy
- Record keeping obligations under Article 30:

  Keep a record showing the name and contact details of the Parish, purposes of processing, categories of data subject and personal data, categories of recipient, international transfers, retention periods, and information security measures in place

- Reporting obligations to the Information Commissioner’s Office (ICO) and data subjects

Privacy by design and by default and DPIAs

- Privacy by design and by default or “think data protection”: This means technical and organisational measures to integrate data protection principles and to demonstrate that you have done so
- Data Protection Impact Assessments (DPIAs) required for “high risk” activities:
  - Document: what you are planning to do; an assessment of necessity and proportionality; the risks; and the measures taken to address those risks
  - May need to consult with individuals and ICO in certain circumstances
- What does this mean in practice? An example of a new computer system

An example of a new computer system

- We can use the new system to set access permissions so that access to information is limited to “need to know”
- The new system will help us keep data up-to-date because everything is going to be stored in one place
- Because everything is stored in one place it will make it easier to delete the data at the right point in time
- The new system will encrypt data automatically. It also requires everyone to have their own username and password.
- Because the system will be used to store most of our data we have decided to carry out a privacy impact assessment

Training, policies and procedures

- All:
  - General training on key data protection issues with a focus on information security
  - Specific role based training
  - A policy covering practical data protection issues
- Internal policies and procedures should include data retention policy; breach management policy and procedure; “special category policy document” (subject to Data Protection Bill clarification)

Agreements with contractors

- Using contractors (data processors) such as payroll providers, and cloud storage providers:
  - Make sure there is a written contract in place which contains the mandatory wording
  - Carry out due diligence / obtain guarantees around data protection and information security
  - Extra rules when transferring data outside of the EEA

Sharing data with other organisations within the community

- A multi Parish benefice would be an example of this. As would sharing data between the Parish and an Incumbent
- Make sure the sharing is covered in the privacy notice
- Keep a record containing some basic rules around sharing such as:
  - What information is shared
  - Information security
  - How to deal with complaints and requests

Part 2:
Privacy notices

Privacy notices

- Must tell individuals how their data is used (usually through a privacy notice). This includes:
  - what their personal data is used for;
  - data subject rights;
  - right to complain (e.g. to the ICO); and
  - grounds for processing (see next slide)
- A “layered” approach to privacy notices
- Privacy notice obligation applies to all those you hold data about
- An example: www.parishresources.org.uk/gdpr/privacy

Part 3: Consent

Consent

- Only get consent if you really have to.
- Consent looks different under GDPR. It must be:
  - Freely given
  - Specific (eg, use lots of tickboxes)
  - Informed (include a detailed description on the consent form)
  - Unambiguous (use clear language)
  - Explicit
- An individual can withdraw their consent
- When do we need consent?

Examples

- Sending anniversary cards (eg, from weddings and baptisms)
- Following up after a funeral to provide ongoing support
- Sending out the Parish newsletter

Part 3: Data security

Examples of breaches

- Misplacing a laptop
- USB sticks being lost or stolen
- Sending a confidential attachment containing personal data to the wrong email recipient
- Leaving confidential documents containing personal data on a doorstep
- Using cc to send emails to multiple recipients

Information held on a computer

- Appropriate technical measures in place to secure your systems
- Who can access the information
- Rules around where files and information should be saved.
- Passwords
- Understand where on the Parish's systems information is stored
- Sending emails to multiple recipients

Paper files

- Keep papers under lock and key in a secure location
- Dispose of paper records securely
- Printing
- Keep a tidy desk
- Sending items in the post - use a courier if sensitive or confidential

Paper files

- Do you need to keep all paper files? Do they duplicate what is held electronically?
- Check what security is in place. For example, kept under lock and key in a secure location?
- Who can access the information?
- Where are paper files kept? E.g. are they stored centrally or do staff and clergy each have their own files?

Homeworking from home and working “on the go”

- Working from home:
  - Information should be kept secure. For example, via encryption
  - Keep papers in a locked case
  - Be aware of surroundings
  - Storage

Information security: Specific GDPR requirements

- Encryption and pseudonymisation
- Keeping data confidential and data resilience (e.g. protection from hackers)
- Backups
- Testing and assessment

When things go wrong

- Step 1: Take immediate steps to “contain” the breach. For example, shut down IT systems
- Step 2: Minimise risk of harm to individuals (e.g. fraud protection)
- Step 3: Consider reporting if appropriate, e.g. to
  - the ICO – GDPR: must report within 72 hours
  - data subjects – GDPR: must inform if “high risk”
  - Insurers
  - Charity Commission for PCCs
- Step 4: “Lessons learnt” and preventing a reoccurrence, both from a technical and procedural point of view

Part 4: Individuals' rights

Individuals' rights

- The GDPR will enhance existing rights and give individuals new rights.
- These rights can be particularly complex to deal with.
- Often made in the context of a complaint or grievance.
- You should know how to recognise when a right is being exercised.

Subject access requests

- A request in writing for an individual's personal data or their child's personal data e.g. "Please send me a copy of all the information you have about me".
- Does not need to mention data protection, personal data or be labelled as a subject access request.
- Personal data disclosable subject to various exemptions.
- No exemption for embarrassing comments.
- Store personal data in such a way that it can be easily searched for if a subject access request is received.

Other GDPR rights

- The GDPR will enhance existing rights and give individuals new rights in their data:
  - Right to be forgotten – individuals can request deletion of their personal data but likely to have limited impact around a your core activities
  - Right of restriction – limited right to “freeze” how you use personal data
  - Right of data portability – applies to information obtained from data subject where relying on consent or necessary for contract
  - Limited right to object
- Staff and clergy should be told how to spot requests
- Staff and clergy should be told to not put anything unprofessional in emails

Part 5:
Sharing and managing information

Sharing information internally

- Data protection legislation applies to sharing information internally.
- Only share information on a “need to know” basis.
- Consider technical measures to prevent access e.g. access permissions, information management software.
- Seniority does not give an automatic right to information.

Sharing information externally

- Data protection does not prevent sharing information for safeguarding reasons
- Be on your guard when an external party asks for personal data.
- Obtaining information by deception does happen, e.g. blagging, phishing and spoofing.
- Telephone – double check number and call back.
- Email – have they used the email address before?
- In person – do you recognise them?

Sharing information externally

- Is the sharing covered by the relevant privacy notice?
- Would the individual expect their personal data to be shared in this way?
- Is the request unusual (e.g. from the Police)?
- If sharing with a service provider there must be a contract in place – see above slide
- Only share what is necessary (e.g. remove information about third parties if not relevant).
- Share securely e.g. encrypted email.

Retention

- Starting point is you should only be keeping information for as long as you need it for the purposes for which it is collected
- See http://www.lambethpalacelibrary.org/content/recordsmanagement but may need to be updated for GDPR
- Independent Inquiry Into Child Sexual Abuse (IICSA). Formerly Goddard Inquiry
- How retention relates to the “right to be forgotten”

Andrew Gallie
Partner
agallie@vwv.co.uk

vwv.co.uk | Offices in London, Watford, Bristol & Birmingham
Lawyers & Parliamentary Agents