THE REPRESENTATIVE CHURCH BODY

PERSONAL DATA BREACH OVERVIEW

© D.Fletcher for CloudTweaks.com

A personal data breach is an incident where information is stolen or taken from a Parish, or Diocese without permission or consent.

All those processing personal data are responsible for protecting it. The regulation states that appropriate policies and technology must be in place to keep the data safe and protect it against ***unauthorised or unlawful processing and against accidental loss, destruction or damage***.

Personal data breaches can include:

- Access to personal information by someone outside the parish without consent from the individual
- Deliberate or accidental action (or inaction) by the parish
- Sending personal data to an incorrect recipient in error
- Computing devices containing personal data being lost or stolen
- Changing personal data without permission
- Loss of personal data

> An example of loss of personal data can include where a device e.g. a laptop containing a copy of a parish's member details, has been lost or stolen.

Data breaches, particularly those most severe, can lead to infringements and penalties and individuals, under GDPR, have the right to claim compensation for any damage suffered as a result of a violation of GDPR.

How to prevent a data breach
Data Breaches often happen because of human error. People can make mistakes. For example, an email containing sensitive information is sent to the wrong person; disposal of records is not done securely; a USB key or laptop is lost.

Necessary measures should now be put in place now to prevent a data breach. For example:

- Have strong passwords on your devices e.g. laptop, computer, phone
- Limited access / permissions to files on the computer to only those who need it
- Lock filing cupboards containing personal data and limit those who have access to the key
- BCC all group emails (blind carbon copy)
- Don't hold onto any personal information you no longer need

Planning for a data breach:
Each Diocese and Parish needs a data breach plan. The plan should include the following steps:

Steps

1. **Leadership:** agree the person in charge of managing the data breach
2. **Identification:** Know how to recognise a data breach
3. **Risk to individuals:** Rate the level of risk

> **'Low risk' example:** Your parish operates a numbered envelope system for donations to the Sunday collections. The only copy of the file linking numbers to parishioners' names is held by the Treasurer. The file is lost. However, the file only contains a code, not any identifying information. The list is meaningless to everyone but the Treasure. In this case it is unlikely to result in a high risk to the rights and freedoms of those individuals. They don't need to be informed about the breach.

'High risk' example: A group from the Diocese goes on a trip to The Holy Land. The trip organiser carries with them a file containing photocopies of the passports of each of the group members. When they arrive home, they realise that this folder is missing. This is likely to result in a high risk to their rights and freedoms, so the individuals would need to be informed about the breach. Following this, the supervisory authority should be contacted, along with the PSNI / An Garda Siochana and the Passport Office.

4. **Contain the breach:** Limit the risk of negative impact. E.g. if you send an email containing Rebekah's personal details to the wrong person by mistake, contact that 'wrong' person and ask them to delete that email immediately. Let Rebekah know what happened and what you have done to contain the breach.

5. **Planning & Communicating:** You need to plan who you contact, and the order in which you contact people. Also, timing is really important. If you have identified that the breach poses a high risk to the data subject you might have to contact the supervisory authority. You have 72 hours to do this once you have identified the breach.

Develop a list of everyone impacted by the breach. It may include:	Develop a list of who else should also be contacted. It may include:
• Members of the Parish • Staff working for the Parish • Members of the Clergy • Members of the Diocese	• Data Protection Officer, RCB • Bishop, Dioc. Secretary • PSNI / An Garda Siochana • Data Protection Supervisory Authority

Before you contact them make sure you know what you are going to say. Individuals will want to know:

- Who is in charge
- What happened
- What is the risk to their personal identity
- What is being done to contain the risk
- What you need them to do
- What are the next steps

Note: If you are contacting the supervisory authority there is information on their website about the information they require. They will want to know what you have done so far, so be proactive.

6. **Analysis of the Breach:** Once the breach has been contained you need to investigate it. See what happened, understand why it happened. If it is a breach that happens regularly, understand why and put a plan in place to prevent this happening again. Keep a log of all data breaches

7. **Damage Control:** You need to ensure you manage all communications very well, be as proactive as you can be and maintain an open door for those who may be concerned with the incident.

8. **Lessons Learnt:** once the breach has been contained and is closed, it is useful to evaluate what happened. With those involved identify what went wrong, how it went wrong, why it went wrong, where it went wrong. Ask if a data breach could have been prevented and look at what new actions and measures need to be put into place to ensure this doesn't happen again. Document this process and save in your GDPR file.

Accountability and Record Keeping:

The parish must keep documentation of all breaches. This record should include: its causes, what took place and the personal data affected. It should also include the effects and consequences of the breach, along with the remedial action taken by the parish.