**Memo on what to do in the event of a Data Breach**

For the first time, GDPR makes it mandatory to notify the ICO of what is called a ‘notifiable data breach’. The penalties that the ICO can levy on an organisation which fails to do this are very heavy, so this is a procedure that churches need to begin getting used to now, before the GDPR comes into force on 25th May 2018.

A data breach is a breach of security leading to the accidental or unlawful destruction, loss , alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. In plain terms, it means an event in which whoever or whichever person or body is processing personal information at the time has lost control of that data in some way………here are some example of situations that could give rise to a data breach:

* 1. an unauthorised person may have gained access to personal data;
  2. personal data (including copies and backups of it) has been lost, even if temporarily;
  3. data has been uploaded onto an unsecure server, including a server situated outside the EEA if this is not done in accordance with the relevant GDPR requirements;
  4. a computer or other device on which personal data is accessible is affected by a virus or other malicious code;
  5. personal data becomes corrupted or is accidentally altered;
  6. any login details were discoverable for a period of time;
  7. a direct marketing email is sent in a manner which allows recipients to view the email addresses of others;
  8. a power outage or other similar incident results in personal data not being accessible for a period of time.

When a member of church staff or volunteer with access to personal data becomes aware that a data breach of **any sort** has occurred, they **must notify** the person designated as the Data Protection Contact Point for the church **as soon as possible by telephone.** In addition, the staff member or volunteer concerned  needs to **quickly follow up that telephone call with an email** detailing the breach on a form similar to the example form headed ‘Internal Data Breach Report Form’ below

**It is the responsibility of the church DP Contact Point person to then decide if the breach is notifiable to the ICO** and if so, the notification must be made on the most up to date version of the form headed ‘ICO. Data protection breach notification form’, which can be accessed from the ICO website.

The notification must include the following information:

1. A description of the personal data breach including the categories of and number of data subjects and records concerned;

(b)The name and contact details of the person appointed as the church’s DP Contact Point and other persons from whom the ICO can obtain more information;

(c)The likely consequences of the data protection breach;

(d)The measures taken or proposed to be taken to address the personal data breach, including measures to mitigate the possible adverse effects.

This notification **MUST BE DONE** within 72 hours of the staff member or volunteer becoming aware of the breach.

Notes:

(i)Time is of the essence here, as this timescale is as stated and no allowance is be made for weekends or public holiday dates;

(ii) it is better to notify a breach in time even if it turns out later that no harm has actually be done; and

(iii) it is better to do a partial notification within the time deadline – this is acceptable to the ICO and it can be followed up later with further detail.

A notifiable breach is one where it is likely to ‘result in a risk to the freedoms and rights of natural persons’. If the resultant risk to these freedoms and rights is high, then the data subjects themselves must also be notified.

Remedial action must be taken immediately after the church becomes aware of a breach. Further, the church must keep an ongoing  register of the occurrence of every data breach and the action taken to remedy same, all as detailed on the suggested example form headed ‘Data breach Record Form’ below.

**Internal Data Breach**

**Report Form**

**STEP 1 –** Telephone ???????? as the church’s the Data Protection Contact Point **immediately**

**STEP 2 –** Complete and email this form to ????????????? as soon as possible. The covering email should be marked ‘Urgent/High Priority’

|  |  |  |
| --- | --- | --- |
| **Report prepared by:** | |  |
| **Date:** | |  |
| 1 | **Summary of the event and circumstances** |  |
| 2 | **Type and amount of personal data**  (*what personal information is included*) |  |
| 3 | **Actions taken by recipient when they inadvertently received the information** |  |
| 4 | **Actions taken to retrieve information and respond to the breach**  (*Has information been retrieved? Has loss been contained? E.g. all emails deleted*) |  |

**Data Breach Record Form**

|  |  |  |
| --- | --- | --- |
| **Report prepared by:** | |  |
| **Date:** | |  |
| **One behalf of:** | |  |
| 1 | Summary of the event and circumstances |  |
| 2 | Type and amount of personal data |  |
| 3 | Actions taken by recipient when they inadvertently received the information |  |
| 4 | Actions taken to retrieve information and respond to the breach |  |
| 5 | Procedures/instructions in place to minimise risks to security of data |  |
| 6 | Breach of procedure/policy by staff member |  |
| 7 | Details of notification to affected Data Subject  Has a complaint been received from Data Subject? |  |
| 8 | Details of Data Protection training provided: |  |
| 9 | Procedure changes to reduce risks of future data loss |  |
| 10 | Conclusion |  |