DATA PROTECTION POLICIES HANDBOOK

Diocese of Galway, Kilmacduagh & Kilfenora

Foreword

The Catholic Church recognises that good pastoral care and respect for the dignity of every person requires that personal data should be sourced, stored, processed and eventually disposed of in an appropriate manner and welcomes the essential principles underlying the General Data Protection Regulation (GDPR) 2018.

Important Terms and Concepts

Personal Data is understood as "any information relating to an identified or identifiable natural person".

Data Processing refers to any activity undertaken involving interaction with a Data Subject's personal data. Data subjects are afforded far-reaching rights under data protection legislation.

A **Data Subject** is the natural person whose personal data is being processed.

The **Data Controller/Data Processor** is the person or organisation involved in data processing activities. A large amount of responsibility is imposed on data processors and controllers under data protection legislation.

Informed, explicit and unambiguous consent is required in order for us to process personal data, unless we are, for example, processing data in the legitimate interests of our diocese. Where contact with a parishioner falls outside of this – e.g. an email address given for the parish readers' rota is used to contact a parishioner about an upcoming fundraising event – we have fallen outside the scope of legitimate interest and must instead seek the explicit consent of the parishioner to gather and use their contact details. Data subjects are entitled to withdraw their consent at any time.

We define retention periods to determine how long we can store personal data in our diocese. During annual reviews, retention periods apply to hard and soft copies of all documents and files, as well as any back-ups which may exist. This means that archives and old storage devices/locations are also subject to the annual review.

Under current legislation, all data subjects have the right to erasure, more commonly known as the 'right to be forgotten'.

If you are in doubt as to the potential data protection implications of a task you are about to undertake, please complete a data protection impact assessment in order to determine your next steps.

A data breach occurs where a breach of security leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data which we as a diocese have transmitted, stored or otherwise processed.

When a data subject submits a subject access request to receive a copy of all the information we hold on them, we must respond within one month of receiving their request. If information relating to the data subject references a third party we may not be required/allowed to disclose.

Data Protection in the Diocese

Data protection is embraced at all levels across our diocese. In our day to day activities, the following activities ensure that we are data aware and data compliant:

Consent

- All application and registration forms for lay ministry, fundraising activities, pilgrimages, etc., will now include a paragraph on consent, which will also mention how the parishioner can 'opt out' of receiving communication.
- Where a parish/diocese can categorically say that they will not contact a parishioner for any other reason than that for which they have signed up, they do not have to gather consent. However, all instances where a parishioner's name is published, e.g. website or parish newsletter will require consent.

Contracts and third parties:

- Absolutely all third-party service providers and contractors must comply with current data protection legislation.
- When engaging in contract negotiations with any third parties who will be processing personal data on behalf of the parish or diocese, it will be ensured that they take a rigorous and proactive approach to maintaining data security.
- Contracts and Service Level Agreements (SLAs) must feature a paragraph on data protection to ensure our and our contractors' compliance with legislation.

Computers and laptops:

- Only suitable authorised persons have access to files and databases containing personal data. Where employees or volunteers carry out their work externally, due care must still be taken in relation to the security of personal data.
- Access rights to files and databases containing personal data are regularly reviewed and updated.
- Passwords in use are unique and are not shared.
- Files are saved in suitable folders, protected where necessary and not readily accessible (e.g. not saved on desktop).
- Computers are regularly locked when unattended or not in use. (For PCs using Windows, a handy shortcut to lock the machine is pressing and holding the Windows key while pressing L).
- Email addresses which are used are those that have been assigned to them, avoiding unsafe platforms like Gmail or Yahoo.
- Email signatures feature a confidentiality disclaimer.
- Printouts containing personal data are disposed of by shredding only.
- Files containing personal data are regularly checked for accuracy and relevance. Any personal data which is no longer in use should be removed from files. Personal data should only be retained for a period of time that is perceived to be reasonably necessary. Retention of personal data on a 'just in case' basis poses a risk to GDPR compliance.

- Parish and diocesan websites must include a comprehensive and up to date privacy policy.
- Where databases and software solutions are provided by third party contractors, compliance is guaranteed through the service level agreement.

Accounts:

- Only authorised persons shall have access to files in the accounts department. Where employees or volunteers carry out their work externally, due care must still be taken in relation to the security of personal data.
- Retention periods for files kept in the accounts department should be in line with Revenue requirements (see Payroll/Personnel Files below).
- Access to accounts files will be physically restricted by means of secured storage, e.g. locked filing cabinets or combination safes.
- Information relating to financial contributions received will be treated in the strictest confidence to avoid potential data breaches.
- Invoices/bills/purchase orders must be kept for a minimum of 6 years before being destroyed in line with Revenue requirements. Please note that this means six years after the transaction or project has been completed as opposed to started.
- Monthly/annual reports sent from parishes to the diocesan accounts department will be password protected and/or saved into a secured shared folder.
- Where accounts are managed by means of a software system, care should be taken to regularly change passwords in order to avoid unauthorised access. This is particularly important when employees/volunteers have external access to accounts e.g. from their own home.

Buildings, Property and Projects:

- Deeds and documents relating to property in the parish or diocese's portfolio are retained by the diocese. Access to these documents will be physically restricted by means of secured access, and only authorised persons shall have access to these files.
- Documents relating to ongoing or past building projects in the diocese shall be subject to the following retention periods:
    - Tender documents, contracts and agreed specifications for minor and repair works to existing buildings should be retained for 6 years after completion of works.
    - All documents relating to major building works should be retained indefinitely and transferred to the diocesan archive.
    - Any documents relating to parish boundaries should be retained indefinitely and transferred to the diocesan archive.

Payroll and Personnel Files:

- Due to the sensitive nature of personnel file content, only authorised persons shall have access to personnel files, e.g. only the parish priest will have access to the personnel files for his parish.
- Where employees or volunteers carry out their work externally, due care must still be taken in relation to the security of personal data.

- Access to personnel files will be physically restricted by means of secured storage, e.g. locked filing cabinets or combination safes.
- An annual check of the content of all diocesan/parish personnel files will be undertaken by the relevant authorised persons.
- The following retention periods will apply to personnel file contents:
    - Application details for candidates who were unsuccessful in a recruitment campaign should be kept for 12 months from date of rejection.
    - Terms and conditions of employment must only be retained for the duration of employment. These records should be kept for no longer than 12 months after the cessation of employment.
    - Payslips/proof that an employees was paid in line with the national minimum wage should be kept for 6 years after cessation of employment.
    - Records of weekly worked hours, the name and address of employee, the employee's PPS numbers and a statement of their duties as prescribed under the Organisation of Working Times Act 1997 should be kept for 3 years after cessation of employment.
    - Records relating to employees who were under the age of 18 (if applicable) for the period of their employment should be retained for a period of 3 years after cessation of employment.
    - In cases of collective redundancies (if applicable), records should be retained for 3 years from the date of redundancy.
    - Where an employee avails of parental or force majeure leave during the course of their employment, the Parental Leave Acts 1998–2006 provides for retention of records for 8 years from cessation of employment.
    - Employee tax records must be kept for 6 years from cessation of employment.
    - Signed confidentiality agreements should be kept for 6 years from cessation of employment.
    - Where an employee is involved in a workplace accident, records of this should be kept for 10 years from cessation of employment.
- A common sense approach will also be taken. Personnel files should contain only factual information pertaining to a person's employment, and should not contain any notes or subjective opinions in relation to any of the records mentioned above.

Child Safeguarding Files:

- Only authorised persons shall have access to safeguarding information, e.g. the Bishop, Chancellor, Director of Safeguarding and Designated Liaison Officer.
- Access to the files will be physically restricted by means of secured storage, e.g. locked filing cabinets or combination safes. This same level of security is applied to all Safeguarding related documents in archives.
- Safeguarding records are held in perpetuity. This includes the information recorded in each parish's sacristy register.
- In general, a common sense approach must be taken to the contents of documents related to safeguarding. These records should contain only factual and relevant information, and should not contain any personal notes or subjective opinions.

- An annual check of the content of all diocesan/parish safeguarding records will be undertaken by the relevant authorised persons.

Parish Files and Records:

- Only authorised persons shall have access to files containing personal data at a parish level, e.g. the parish priest and/or secretary.
- Access to these files will be physically restricted by means of secured storage, e.g. locked filing cabinets or combination safes. Particular care will be taken in relation to Safeguarding files.
- An annual check of the content of files containing personal data will be undertaken by the relevant authorised persons. This content check will ensure that information held in each parish is relevant, accurate and not being retained for longer than necessary.
- The following retention periods will apply to parish files and records – every effort will be made to keep this list accurate and up to date:
    - Safeguarding files, e.g. application forms: held in perpetuity.
    - Parish sacramental registers: parish sacramental registers have a permanent reference and should be held in perpetuity.
    - Sacramental application forms: sacramental application forms are intended for the purpose of facilitating sacramental preparation, celebration and registration, and have no purpose once the sacrament has been celebrated and registered. They should be destroyed within 12 months of celebration.
    - HR/personnel files: See policy on personnel file management for specific information.
    - Contact details and other personal data of lay ministers, fundraisers, etc.: these should only be retained for as long as the parishioner is engaged in ministry or other activities on behalf of the parish.
    - Minutes from meetings: meeting minutes should only contain a factual account of what was discussed and agreed during a meeting, without referring to opinions expressed by individuals. Minutes should be kept for as long as is deemed reasonably necessary. During the annual content check, the authorised person for the parish/diocese should use their judgement to decide on this. Keeping minutes on a 'just in case' basis poses a risk to GDPR compliance.
    - Records of one to one meetings: insofar as is possible, apply the same logic as above.
    - Records of contributions and donations: these should be anonymised insofar as is practical, and access to contributor details should only be assigned to authorised persons. These details should be kept for as long as is deemed reasonably necessary, giving due consideration to Revenue requirements.
    - Correspondence to and from parishioners or others about the activity of the parish: details of correspondence must only be retained where and for as long as is reasonably necessary.

Planned Giving Envelopes:

- Planned giving envelope boxes containing the name and address of a parishioner are effectively an example of sensitive personal data, as they show a person's religious affiliation. As a result, the parish should take reasonable care that this personal data is

protected when the boxes are being distributed. If boxes are collected by parishioners, they should not be left in the church outside of Mass times, but rather locked in the sacristy. If they are distributed by employees or volunteers, ensure they have signed confidentiality agreements with the parish.

- Software and/or files linking planned giving envelope numbers with the name of the parishioner should be password protected and only accessible by suitable authorised persons.

CCTV, Webcams and Livestreaming:

- CCTV recording takes place in order to detect intruders, and will not be used for the purposes of monitoring employees or volunteers.
- All buildings and surrounding areas covered in the scope of CCTV cameras will be clearly outlined on a risk assessment/overview which will be made available upon request.
- Notices will be put in place to inform all potential data subjects of the presence and purpose of CCTV cameras.
- CCTV footage will be retained for a period of 30 days, unless required for the purposes of an investigation.
- Outsourced CCTV services must comply with the above requirements.
- Webcams and live-streaming have been introduced solely as an alternative means for parishioners to enjoy the celebration of Mass and the sacraments. Webcams in churches are not used to monitor employees or parishioners.
- Notices will be put in place to inform all potential data subjects of the presence and purpose of the webcam/s. The scope of the webcam/s will be indicated at the entrance to the church, to afford parishioners the opportunity to opt out of streaming or recording.
- Recordings of a small number of celebrations will be retained for one month, e.g. Christmas. In these instances, the parish priest will make an announce at the beginning of the celebration to ensure the consent of parishioners present. Where children or vulnerable adults are taking part in a celebration, consent and/or parental consent will be sought in advance.
- Outsourced webcam and live-streaming services must comply with the above requirements.

Social Media and Websites:

- Social media sites, e.g. Facebook or Instagram, operated by the parish or diocese should have restricted edit access.
- Posts or photographs which contain personal data must have the prior consent of the data subject before being posted on social media or websites.
- Posts or photographs which contain personal data must be deleted or archived after one year. If the information is archived, suitable location and access must be defined.

Requests for Certificates:

- Copies of certificates held in the parish or diocesan offices can only be requested in writing and registers are not to be made accessible to the public. These written requests should be

destroyed once processed. If you have any doubts regarding the identity of the person requesting the information, reasonable means should be used to confirm identity. The '100-year rule' will be used to reasonably assume whether someone is dead or still protected by data protection legislation.

Subject Access Requests

- Subject access requests (SAR) must be received in writing and referred immediately upon receipt to the Data Protection Officer. If a SAR is made verbally, please advise the data subject to send their request in writing to a suitable postal or email address. The DPO can be informed via phone or email of the SAR, and should be forwarded a copy of the written request as soon as possible. The DPO will then work together with the impacted Diocese / Parish to ensure that the SAR is completed at no cost to the data subject, within one month of receipt. Certain exceptions will apply, whereby the diocese may not be required or legally permitted to release certain data, but this will be discussed and clarified with the DPO and, where necessary, the diocese's appointed legal counsel. If you have any doubts regarding the identity of the person requesting the information, reasonable means should be used to confirm identity.

Right to Rectification

- All data subjects have the right to have their information updated or removed where it is not accurate, provided it will not impact on the rights and freedoms of another natural person. Again, these requests should be received in writing and processed at the earliest convenience. If you have any doubts regarding the identity of the person requesting the information, reasonable means should be used to confirm identity.

Data Protection Impact Assessment (DPIA)

- DPIAs should form the basis for all new processes in the diocese which will involve data processes. DPIAs are similar to risk assessments, in that they will identify the potential challenges posed by implementing new processes, and also identify potential solutions to offset these challenges. The DPO can provide a DPIA checklist.

Data Breaches

- First and foremost, we must all be completely committed to the avoidance under all circumstances of data breaches. Data breaches must be reported to the Office of the Data Protection Commissioner within 72 hours, unless the breach poses no risk to the rights or freedoms of any natural person. Where we do not report the breach within 72 hours, we must inform the Data Protection Commissioner of the reasons for the delay. If you suspect or, even accidentally, cause a data breach, please contact the Data Protection Officer immediately to discuss next steps.
- All third party service providers associated with the Diocese are obliged to comply with this requirement.

Right to Erasure

- All data subjects have a right to be forgotten, where requested. This can pose certain difficulties for the diocese under Canon Law. The right to erasure cannot be invoked in

cases of legal disputes or investigations, e.g. in child safeguarding matters. Where a parishioner, for example, requests to be forgotten by virtue of leaving the Catholic Church, it is our current understanding that we may retain certain factual records, e.g. entries on baptismal records. This may be subject to change following future guidance from the Data Protection Commissioner.

Annual Reviews

- Annual reviews should be completed at times which are practical and convenient for the parish or diocese, but must be completed. To this end, the parish or diocese may choose to split their full annual review over three separate review periods, which is facilitated in the annual review template. The responsibility for full completion will lie with the parish or diocese themselves.

Implementation and Assurance:

- Every effort will be made to ensure adherence to this handbook. To this end, the Data Protection Officer will carry out ad hoc, unannounced visits to parishes in order to provide feedback on the current status of compliance. This is foreseen to begin within 12 months of the initial rollout of the handbook, and will be purely on a support / assurance basis. Earlier visits can be planned with the DPO where additional support with implementation is required. Feedback will be provided by way of a report, which will be provided to the parish priest and bishop/archbishop.

Contact

The data protection officer is the person nominated by the diocese to support all activities in relation to data protection compliance. Barrister Malachaí Ó Dubhda is the current Data Protection Officer and Information Law Consultant for the Western Dioceses. (January 2021.)

Email dpo@elphindiocese.ie