Data Protection Policy

AUGUSTINIAN PROVINCE OF IRELAND

December 2018

Forward:

The Augustinian Province of Ireland has an ethical responsibility to maintain the highest standards of confidentiality in the safeguarding of information about its members, staff members and those individuals, donors, agencies and others that interact with the Province.

Information collection is essential to us fulfilling our duties. Data Protection legislation seeks to give people control of their own personal information and so it confers certain obligations on the Province in relation to how personal information is collected and used. The legislation was originally introduced to protect individual's personal information from misuse by automated means. This has since been extended to include processing of manual data.

The Data Protection Acts of 1988 and 2003 and the General Data Protection Regulations (GDPR) 2018, play a significant role in how we process Personal Data. The aim of this policy is to ensure that each member, staff member and others with whom the Province interacts, has an understanding of the concepts of Data Protection and is aware of their own responsibilities in relation to the Order's overall compliance with the Acts.

John Hennebry OSA

Prior Provincial

Date: December 2018

Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of The Augustinian Province of Ireland. This includes obligations in dealing with Personal Data, to ensure that the Province complies with the requirements of relevant Irish and European legislation, namely the Irish Data Protection Act (1988), the Irish Data Protection (Amendment) Act (2003) and the EU General Data Protection Regulations (GDPR) (2018).

Rationale

The Augustinian Province of Ireland must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed and stored by the Province in relation to its members, staff members, service providers, donors and those individuals, agencies and others with whom they interact in the course of their activities. The Province makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

Scope

The policy covers both personal and sensitive Personal Data held in relation to data subjects by the Province. The policy applies equally to personal data held in manual and automated form.

All Personal and Sensitive Personal Data will be treated with equal care by the Province. Both categories will be equally referred to as Personal Data in this policy, unless specifically stated otherwise.

The Augustinian Province of Ireland As A Data Controller

In the course of its daily organisational activities, the Augustinian Province of Ireland acquires, processes and stores Personal Data in relation to:

- Friar members of the Order.
- Employees of the Province
- Third party service providers engaged by The Province
- Donors
- Volunteers

In accordance with Irish Data Protection legislation and the General Data Protection Regulations (GDPR), this data must be acquired and managed fairly. Not all staff members will be expected to be experts in Data Protection legislation. However, the Augustinians are committed to ensuring that its staff have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In

such circumstances, staff must inform the Provincial Office so that appropriate corrective action can be taken.

Due to the nature of the services and activities of The Augustinian Province of Ireland, there is regular and active exchange of Personal Data between the Province and its Data Subjects. In addition, the Province exchanges Personal Data with Data Processors on the Data Subjects' behalf. This is consistent with the Provinces obligations under the terms of its contract with its Data Processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that an employee of the Province is unsure whether such data can be disclosed.

If in doubt, staff should consult with the Provincial Office to seek clarification.

*****

The Data Protection Principles

The following key principles are enshrined in Irish legislation and are fundamental to the Augustinian Province of Ireland Data Protection policy.

GDPR – May 2018	Irish Data Protection Acts 1988, 2003 & 2018
1. Lawfulness, Fairness & Transparency	1. Obtain and Process Information Fairly
2. Purpose Limitation	2. Keep it for only one or more specified, explicit and lawful purposes
3. Integrity & Confidentiality	3. Use and disclose it only in ways compatible with these purposes
4. Accuracy	4. Keep it Safe & Secure
5. Data Minimisation	5. Keep it Accurate, Complete & Up To Date
6. Storage Limitation	6. Ensure that it is adequate, relevant and not excessive
7. Accountability	7. Retain it no longer than is necessary for the specified purpose or purposes
	8. Give a copy of his/her personal data on request.

In its capacity as Data Controller, the Province ensures that all data shall:

1. ... be obtained and processed fairly and lawfully.

For data to be obtained fairly, the data subject will, at the time of collection, be made aware of:

- The identity of the Data Controller (Augustinian Province of Ireland)
- The purpose(s) for which the data is being collected
- The person(s) to whom the data may be disclosed by the Data Controller
- Any other information that is necessary so that the processing may be fair.

Augustinian Province of Ireland will meet this obligation in the following way.

- Where possible, the informed consent of the Data Subject will be sought before their data is processed;

- Where it is not possible to seek consent, Augustinian Province of Ireland will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Where Augustinian Province of Ireland intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view. The use of CCTV is for security purposes only and will not be used to monitor the work of employees or volunteers.
- Web-streaming will only be carried out for the duration of the Mass time. Fair Processing Notices of Streaming will be posted in full view. Cameras are pointed at the Altar, away from the congregation.
- Processing of personal data will be carried out only as part of Augustinian Province of Ireland's lawful activities, and the Province will safeguard the rights and freedoms of the Data Subject;
- The Data Subject's data will not be disclosed to a third party other than to a party contracted to the Augustinian Province of Ireland and operating on its behalf.

2. .... be obtained only for one or more specified, legitimate purposes.

The Augustinian Province of Ireland will obtain data for purposes which are specific, lawful and clearly stated. A Data Subject will have the right to question the purpose(s) for which the Augustinian Province of Ireland holds their data, and the Province will be able to clearly state that purpose or purposes.

3. ..... not be further processed in a manner incompatible with the specified purpose(s).

Any use of the data by the Augustinian Province of Ireland will be compatible with the purposes for which the data was acquired.

4. .... be kept safe and secure.

The Augustinian Province of Ireland will employ high standards of security in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorized access to, or alteration, destruction or disclosure of any personal data either manual or electronic held by The Province in its capacity as Data Controller. Access to and management of personal data is limited to those who have appropriate authorization and password access. Administration staff are asked to keep emails and computer files password protected and with limited access.

5. ... be kept accurate, complete and up-to-date where necessary.

The Augustinian Province of Ireland will:

- ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
- conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. The Province conducts a review of sample data annually to ensure accuracy; Staff contact details and details on next-of-kin are reviewed and updated every two years.
- conduct regular assessments in order to establish the need to keep certain Personal Data.

6. ... be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed.

The Augustinian Province of Ireland will ensure that the data it processes in relation to Data Subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

7. ... not be kept for longer than is necessary to satisfy the specified purpose(s).

The Augustinian Province of Ireland has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format. Once the respective retention period has elapsed, The Augustinian Province of Ireland undertakes to destroy, erase or otherwise put this data beyond use.

8. ... be managed and stored in such a manner that, in the event a Data Subject submits a valid Subject Access Request seeking a copy of their Personal Data, this data can be readily retrieved and provided to them.

The Augustinian Province of Ireland has implemented a Subject Access Request procedure to manage requests in an efficient and timely manner, within the timelines stipulated in the legislation. (30 days on receipt of application - *GDPR 2018*)

Data Subject Access Requests

As part of the day-to-day operation of the organisation, Augustinian Province of Ireland's staff engage in active and regular exchanges of information with Data Subjects. Where a formal request is submitted in writing by a Data Subject in relation to the data held by the Province, such a request gives rise to access rights in favour of the Data Subject.

There are specific time-lines within which the Province must respond to the Data Subject, depending on the nature and extent of the request. These are outlined in the Subject Access

Request Form available on our website or on request from the Augustinian Provincial Office.

The Province's staff will ensure that, where necessary, such requests are processed as quickly and efficiently as possible, but within not more than 30 days from receipt of the request.

Third-Party Processors

In the course of its role as Data Controller, the Augustinian Province of Ireland engages a number of Data Processors to process Personal Data on its behalf. In each case, a formal, written contract is in place with the Processor, outlining their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with Irish Data Protection legislation (1988) and (2003) and the General Data Protection Regulations (2018).

These Data Processors may include:

- IT Services
- Payroll & Accounts Services
- Pensions & Investment Services
- HR Services

Implementation:

As a Data Controller, The Augustinian Province of Ireland ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

Failure of a Data Processor to manage The Augustinian Province of Ireland's data in a compliant manner will be viewed as a breach of contract and will be pursued through the courts by the Province.

Failure of the Province's staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

What Constitutes A Breach, Potential or Actual?

A breach is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons

other than authorized users, for an authorized purpose, have access or potential access to Personal Data in usable form, whether manual or automated.

This could mean:

- Loss of a laptop, memory stick or mobile device that contains Personal Data
- Lack of a secure password on pc's and applications
- Emailing personal data to someone in error
- Giving a system login to an unauthorised person
- Failure of a door lock or some other weakness in physical security which compromises personal data

What Happens If A Breach Occurs?

Actual, suspected, or potential breaches should be reported immediately to the Augustinian Provincial Office – 01-4851516 or provincialoffice@augustinians.ie

The Provincial Office will assess the breach and determine its severity. Depending on the scale and sensitivity of data lost and the number of Data Subjects impacted, the Office of the Data Protection Commissioner and relevant regulatory bodies will be informed as quickly as possible following detection.

In certain circumstances The Augustinian Province of Ireland may (e.g. if required by the Office of the Data Protection Commissioner), inform the data subjects of the loss of their data and provide them with an assessment of the risk to their privacy. The Province will make recommendations to the data subjects which may minimise the risks to them. The Province will then implement changes to procedures, technologies or applications to prevent a recurrence of the breach.

Definitions:

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data	This includes both automated and manual data. Automated data means data held on computer or stored with the intention that it is processed on computer. Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Personal Data	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other

	data which is likely to come into the legitimate possession of the Data Controller.
Sensitive Personal Data	A particular category of Personal data, relating to: racial or ethnic origin, political opinions, religious, ideological or philosophical beliefs, trade union membership, information relating to mental or physical health, information in relation to one's sexual orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.
Data Controller	A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.
Data Subject	A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
Data Processor	A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

Appendix 1 – Data Subject Access Request Form

Appendix 2 – Retention Schedules (Augustinian Province of Ireland)

APPENDIX 1

DATA SUBJECT ACCESS REQUEST FORM

Full Name:

_____

Address: _____

_____

Telephone:

_____

Email:

_____

Are you the Data Subject?

If YES; please supply evidence of your identity, i.e., something bearing your signature such as a copy of driving licence or passport.

If NO, and you are acting on behalf of the Data Subject, please provide us with their written authority.

Please provide us with their…

Full Name: _____

Address: _____

Telephone:_____

Email: _____

Please describe your relationship with the data subject that leads you to make this request for information on their behalf

Please describe the information you seek together with any other relevant information. This will help to identify the information you require

DECLARATION:

To be completed by all applicants. Please note that any attempt to mislead may result in prosecution.

I…… certify that the information given on this application form to the Augustinian Province of Ireland is true. I understand that it is necessary for the Province to confirm my/the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct Personal Data.

Signature:_____

Date: _____

A response to an Access Request will be supplied to the individual within 30 days of receiving the request.

Please return the completed form to…

Provincial Office,

Augustinian Province of Ireland

Taylor's Lane,

Ballyboden,

Dublin 16 D16YN32

Documents which must accompany this application include…

- Evidence of your identity
- Evidence of the data subject's identity (if different from above)
- Authorisation from the data subject to act on their behalf (if applicable)

Please include a stamped addressed envelope for return of proof of identity.

Appendix 11

Records Retention Guide 2018:

Current Records (in office)

General Administration	1 year approx.. then send to storage
Accounts/Finance	1 year approx.. then send to storage

Non-Current Records (storage)

General Administration	3 years then either dispose, or, if historically interesting, send to archives
Accounts/Finance	7 years then dispose or send to archives
Human Resources	1 year for unsolicited applications
	1 year post termination
	2 years applications and interviews
	3 years hours/annual leave
	5 years work permit
	7 years pay records (see accounts/finance)
	8 years carers leave/parental leave etc.
Garda Vetting	4 Years – (Duration of Vetting Process)

Safeguarding	Files relating to Criminal Investigations have no retention schedule and are retained on a permanent basis.