BISHOPS' CONFERENCE OF SCOTLAND

DATA PROTECTION POLICY

Table of Contents

Document Control

Title	Data Protection Policy
Prepared by	Donna Maguire
Approved By	
Date of Approval	
Version Number	1.2
Review Frequency	Every 5 years
Next Review Date	

Status Control

Version	*Date*	*Status*	*Prepared by*	*Reason for Amendment*
1.2	11/2/2018	Draft	DMM	

1 INTRODUCTION

The Bishops' Conference of Scotland (also known as the Catholic National Endowment Trust, CNET, and referred to as 'BCOS' in this document) is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR) 2016 ('the Regulation'), which will come into force on the 25th of May 2018, (and will be realised in the Data Protection Bill 2017, once it has passed through Parliament.) This follows on from the Data Protection Regulation 1998, which came into force on the 1st March 2000. BCOS will follow procedures that aim to ensure that all BCOS employees, contractors, agents, consultants, partners, volunteers or others who have access to any personal data held by or on behalf of the BCOS, are fully aware of and abide by their duties and responsibilities under the Regulation.

2 BACKGROUND INFORMATION

The GDPR 2016 (once it becomes the Data Protection Bill 2017) broadens and enhances the scope of the Data Protection Act 1998, following on from the Data Protection Act 1984. Its purpose is to protect the rights and privacy of natural persons and to ensure that personal data is not processed without their knowledge, and wherever possible, is processed with their consent.

2.1 Definitions

- **Data Protection Officer –** is employed to assist in the monitoring of internal compliance.
- **Data Controller –** Organisation or individual who determines why or how personal data is to be processed.
- **Data Processor –** Person who processes the data in accordance with the processes and security measures determined by the data controller.
- **Data Subject –** Any natural person who is the subject of personal data held by an organisation.
- **Personal Data –** Any information relating to an identified or identifiable data subject. An identifiable Data Subject is one who can be identified, directly or indirectly, by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This can also include credit/debit card number, telephone number, eye colour, job title, religion, IP address, and photographs.
- **Special Categories of Personal Data –** The same as personal data with the following additions: special categories of personal data include racial/ethnic origin; political opinions; religious beliefs; philosophical beliefs; trade union membership; genetic data; biometric data; data relating to health; sexual orientation; and details of sexual history.

N.B. The processing of special categories of personal data is prohibited under the GDPR except for the following specific conditions:

- where the Data Subject has given explicit permission
- where processing is necessary for obligation of the Data Controller in the fields of employment, social security and social protection law
- processing is necessary for vital interests of the Data Subject where consent cannot be given
- processing relates to personal data which have been made public by the Data Subject
- processing is necessary for substantial public interest
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in a judicial capacity

2.2 Organisational Responsibilities

2.2.1 Primary responsibility for ensuring organisational compliance with the Regulation rests with the employer.

2.2.2 The Data Controller must provide the data processors with a policy and/or guidelines for collecting and processing personal data.

2.2.3 The Data Controller must ensure that the data processors understand the policy and/or guidelines and are aware of their responsibilities.

2.2.4 The Data Controller should monitor compliance with the Regulation.

2.2.5 Data processors are responsible for collecting and processing personal data according to the policy and/or guidelines issued and training provided by the Data Controller.

2.3 Principles of Data Protection

Article 5 of the Regulation stipulates that anyone processing personal data must comply with six principles of good practice. These Principles are ***legally enforceable***.

The Principles require that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

3 BCOS DATA PROTECTION POLICY

The BCOS will handle and process personal data and sensitive personal data according to the following principles:

- Data subjects will be informed of the intended purpose of the information being collected.
- Data will be collected and processed only if it is appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- The quality and accuracy of information used will be maintained as far as possible.
- Implicit consent of the data subject to the collecting, processing and sharing of personal data will not be implied.
- Explicit consent of the data subject to the collecting, processing and sharing of sensitive personal data will always sought.
- Data obtained from third parties will not be used, unless assurances as to the Data Subject's consent has been provided.
- Data will not be shared outside of the EEA, to countries not recognised by the European Commission as having an adequate level of protection, (US organisations not signed up to the Safe Harbour Scheme.) or to countries whose data protection policies are not considered adequate by the Trust.

3.1 Collecting Personal Data

Whenever data is being collected using a form, the statements available in the document 'Templates for Data Collection Forms' should be included.

3.2 Maintaining Personal Data

The BCOS will maintain personal and sensitive data according to the following principles:

- safeguarding the security of data
- taking reasonable steps to ensure the accuracy of data
- providing data subjects with a right of access to their data
- destroying data in an organised and secure manner.

3.3 Security of Personal Data

All employees and individuals are responsible for ensuring that personal data and sensitive personal data which they hold is kept securely and that it is not disclosed to any unauthorized third party.

All personal data and sensitive personal data should be accessible only to those who need it. Employees and individuals should form a judgement based upon the sensitivity and the value of the information in question, but should always consider taking the following precautions:

- storing data in a lockable room with controlled access
- storing data in a lockable filing cabinet
- using passwords to protect electronic data
- storing disks in a lockable cabinet
- using password protected screensavers for unattended PCs.

Personal data must be destroyed by following the procedures in the BCOS Waste Disposal Policy.

NB. In the event of a data breach, you must contact your Line Manager and/or the Data Controller (Donna Maguire) immediately, as the Information Commissioner's Office must be informed within 72 hours of the discovery of a breach.

3.4 Accuracy of Personal Data

The Regulation requires that all reasonable steps are taken to ensure accuracy of data.
The BCOS will:

- apply checks to determine the length of time information is held
- attempt to check data accuracy at regular and appropriate intervals
- inform all relevant third parties of changes to data
- request all third parties to destroy data when appropriate.

3.5 Rights of Access to Personal Data

- Subject Access Request (SAR) – the right of the individual to access data about them, any personal data or sensitive personal data held about them and the right to correct any errors.
- Any individual who wishes to exercise this right should apply in writing to:

  Donna Maguire
  Archivist and Records Manager
  Scottish Catholic Archives
  Columba House
  16 Drummond Place
  Edinburgh, EH3 6PL

Some requests may be able to be carried out at the agency/office level. If so, they must be reported to the BCOS Data Controller (Donna Maguire). This information will then be recorded in the BCOS Information Audit which will be reviewed yearly by the Data Protection Officer. There may also be information on a person that the receiving agency/office is unaware of.

A fee cannot be charged for access to, or copies of, personal data. Any request will be complied with, within 30 CALENDAR DAYS (one month) of receipt of request, unless exceptional circumstances apply.

3.6 Destruction of Personal Data

Data should be reviewed for destruction when its original purpose or justification for collection has ceased to exist. All paper and electronic records containing personal data or sensitive personal data must be destroyed according to the procedures in the BCOS Retention Schedule.

The Archivist may notify the employee or individual responsible for the data when this should occur, but it is the responsibility of the employee or individual to ensure that it is done.

3.7 Inventory of Personal Data

To assist in compliance with the Regulation, the BCOS will establish an inventory of databases and filing systems containing personal data assets, both digital and paper. Employees and individuals responsible for each database or filing system are responsible for informing the General Secretary/Archives Office of the name, location and details of each asset as set out in the BCOS Information Audit Form.

Databases containing sensitive personal data are to be retained by departments, but the name and details of each must still be notified to the General Secretary, Archive and BCOS IT Support.

4 FURTHER INFORMATION

Further advice, guidance and resources on Data Protection and related issues are available in the following documents:

- Basic Guide to Data Protection
- Templates for Data Collection Forms
- Subject Access Request Form
- Retention and Disposal Schedules
- Email Policy
- Use of Personal IT Equipment
- Remote working Policy
- Information Audit Form and Guides.

General information and guidance on Data Protection issues is available from the Archivist, Donna Maguire.

Important Note

If you receive a Subject Access Request, a complaint regarding handling of personal data, any communication which could have legal implications for the BCOS regarding its data handling, or if you are planning a project or activity which will involve collecting or processing personal data in a new way, then you should inform the Archivist, Donna Maguire, before proceeding.