The Church of Scotland

Data Protection Overview

The right to privacy is a fundamental right, enshrined in the European Convention on Human Rights . There have been data protection laws in place for some time, the most recent change being the introduction of the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018. Since the UK is no longer a member of the EU there is now the UK GDPR which is largely equivalent in terms of protecting individuals' rights under privacy laws. This guidance provides an overview of data protection laws and what is required to comply with them.

Data Protection Principles

There are six key data protection principles which must be followed, with an overarching principle of 'Accountability' which requires an organisation (the "controller") to demonstrate its compliance with data protection laws. These require that personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**')
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation**')
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**')
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 ('**accuracy**')
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 ('**storage limitation**')
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 ('**integrity and confidentiality**').

The Accountability principle is that "The controller shall be responsible for, and be able to **demonstrate compliance** with the principles ('**accountability**')."

Data Subject Rights

Individuals (known as data subjects under data protection laws) have a number of rights. These are as follows:

1. The **right to be informed** – a privacy notice in relation to the purpose of processing will address this. This links with Principle 1 – 'fairness and transparency'. An individual should be provided with a privacy notice when their data is collected.
2. The **right of access**, commonly known as subject access request (SAR) – this means an individual has the right to access and receive copies of personal data an organisation holds.
3. The **right to rectification** – this means that if any personal data which is held by an organisation is incorrect or incomplete the individual has the right to correct the data or in the case of incomplete data, provide further detail.

4. The **right to erasure**, commonly known as the right to be forgotten (RTBF) – this means an individual can request all data held about them be deleted by the organisation. Such a request must be considered carefully but need not always be granted.
5. The **right to restrict** – this links with some of the other rights and means an individual can request that the organisation restricts the processing of their personal data while the issue is resolved, for example if the data is incorrect and the rectification right is exercised.
6. The **right to data portability** – this means that an individual has the right to request an organisation to provide their personal data in a machine-readable format, e.g. a .csv file and transfer it to another organisation
7. The **right to object** – this means that an individual can object to the processing and the controller has to stop unless the organisation can prove a legitimate lawful purpose for the processing. The right to object is absolute in relation to marketing purposes.
8. **Automated individual decision-making, including profiling** – Currently the Church does not carry out automated individual decision-making including profiling. However, if this was to change, the individual has the right to request that there is human intervention in the processing rather than it being entirely automated. So, if the Church were to begin doing this type of processing, individuals must be informed and the Church must build into the system a way that the decision making can be made by an individual.

Not all rights are absolute and depend on the lawful basis for processing. The table below provides detail as to what rights apply depending on the lawful basis for processing.

	Lawful Basis for Processing					
Data Subject Right	**Consent**	**Contract**	**Legal Obligation**	**Vital Interests**	**Public Interests/task**	**Legitimate Interests**
Informed	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Access	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Rectification	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Erasure	**Yes**	**Yes**	**No**	**Yes**	**No**	**Yes**
Restrict Processing	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Portability	**Yes**	**Yes**	**No**	**No**	**No**	**No**
Object	**No**	**No**	**No**	**No**	**Yes**	**Yes**
Automated Decisions	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Withdraw Consent	**Yes**	**No**	**No**	**No**	**No**	**No**

The Church of Scotland

Key Data Breach Reporting Requirements

The Church has a number of obligations under data protection laws, as detailed above and in further detail at the Resources section of the Church website. One aspect that is critical is the proactive and timeous reporting of a data breach. If the Church is made aware of a '**personal data breach**' (defined as 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) it has 72 hours to report it to the regulator, the UK Information Commissioner's Office (ICO). If the breach is likely to impact on the rights and freedoms of the affected individuals they must be informed too. The reporting of incidents swiftly is vital, especially considering that the ICO has the power to issue fines of up to **£17.5 million or 4% of annual global turnover** – whichever is greater – for data breaches. It is therefore vital that such breaches are identified and reported to the Church's Data Protection Officer (DPO), Alice Wilson, either directly at Alice.Wilson@churchofscotland.org.uk or Privacy@churchofscotland.org.uk without undue delay and ideally no later than 24 hours.