Data Protection Overview: Blairgowrie Parish Church: January 2024

The UK Data Protection Act 2018 and the UK General Data Protection Regulations recognise the right to privacy as a fundamental human right. This Act and these Regulations are largely equivalent to the European Convention on Human Rights in terms of protecting an individual's right to privacy.

Personal Data

Data Protection relates to personal data and the GDPR defines personal data as: "any information relating to an identified or identifiable natural person (called a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or societal identity of that natural person. Under the current law, the definition relates to living individuals and **to data held electronically or on paper records/in manual filing systems**. The explicit inclusion of location data, online identifiers and genetic data is new, and may result in additional compliance obligations.

The following provides an overview of data protection laws.

Data Protection Principles

There are six key data protection principles and these must be followed. The overarching principle is one of **'Accountability'** which requires an organisation to **demonstrate** its compliance with data protection laws.

Personal data must be:

1. Processed lawfully, fairly and in a transparent manner. **('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 (the organisation) shall be responsible for, and be able **to demonstrate compliance** with the principles."

Data Subject Rights

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

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 (or in the case of the church, given access to) 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.

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. **The right to prevent 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. More information about this is available at GDPR_General_Guidance_for_Congregations2018.pdf

Key Data Breach Reporting Requirements

The Church has a number of obligations under data protection laws. 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. The Information Commissioner's Office has the power to fine organisations up to £17.5 million 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.

How does this affect us?

Examples of church data processing include:

- Staff/payroll records

- Membership lists (Congregational Roll, Guild Membership, Boys Brigade (although the BBs operate under its own organisational data protection rules), Social Club, Craft Group)
- Baptismal records;
- Information relating to pastoral care;
- Information regarding those attending holiday clubs or other activities;
- Lists of children/young people attending Sunday schools, youth groups and creches;
- Records of those for whom the congregation holds contact details for various reasons, including volunteers working with children and young people and others (safeguarding records), those attending churches, making Gift Aid donations, district lists, hall hire details, keyholder/keycode register, electronic newsletter register, etc.
- Personal data can also include digital photographs and videos, where images are clear enough to enable individuals to be identified.

Special Category Data

This special category of personal information replaces the previously used "sensitive personal data" category. It is personal data which are stated to be more sensitive than other types of data, and so require additional protection and safeguards. Special category data is defined as "personal data revealing a person's racial or ethnic origin, political opinions, **religious** or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a person, or data concerning health or sex life and sexual orientation".

Most of the personal data processed by congregations about individuals will come under the definition of special category data, either specifically or by implication, as the mere holding of any information about a person by a congregation is likely to be indicative of that person's religious beliefs.

January 2024