# Data Protection Help Sheet

If your organisation processes and retains personal information regarding individuals, then you need to be aware of what you should be doing to protect that information.

As the Management Committee, you have a responsibility to ensure that your organisation's practices are compliant with data protection laws.

Data protection laws aim to strike a balance between the rights of individuals and the interests of those with legitimate reasons for using their personal information. Individuals, for example, are given the rights to access certain information held on them.

The provisions of the General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA) 2018 govern the use of personal data. The Information Commissioner's Office (ICO) is the data protection supervisory authority (regulator) in the UK.

The Management Committee needs to ensure that the organisation has considered 3 key questions regarding data protection:

1. Does our organisation process personal data?
2. Are we obligated to notify the ICO that we are handling personal information?
3. What principles should govern how we handle personal information and how are we ensuring that our policies and practices are compliant?

## 1. Does your organisation process personal data?

Personal data is information that relates to a living individual who can be identified from those data, or from the data and other available information. The definition covers both facts and opinions about the individual.

Processing covers the use of this personal information. It can include collection, storage, retrieval, analysing, updating, deletion, disclosure, transfer, publication and more.

- If you obtain, record, use or hold such information, then you are considered to process personal information. You therefore need to consider questions 2 & 3.
- If you do not process personal information, then you do not have any obligations under the GDPR or DPA.

You need to keep a written electronic record of the personal data your organisation processes. The ICO has developed basic templates which you can use to help you maintain a register of all the personal information you hold and the purpose that it is used for. These spreadsheets can be downloaded from the ICO website here.

## 2. Are we obligated to notify the ICO that we are handling personal information?

Click here for a self-assessment questionnaire to confirm whether your organisation needs to provide notification.

Those who process personal information are obliged to register with the Information Commissioner that they are doing so and pay an annual data protection fee. However, most not-for-profit organisations will find themselves covered by the exemption.

Source: www.diycommitteeguide.org

Essentially, if you are a not-for-profit organisation and you process personal information solely for the purposes of:

- Maintaining a membership or supporters scheme
- Providing or administering activities for members or individuals who have regular contact with you
- Staff administration, accounts or business activity records
- Advertising, marketing and public relations in connection with your own activities

then you are likely to be exempt from notification. In addition, if none of your processing (including other purposes) is carried out electronically (including computers, smartphones, call recording, etc), then you are unlikely to need to notify, but you are still covered by data protection laws.

However, if you use CCTV for crime prevention then you do have to pay the data protection fee. For registered charities, this is £40 per year.

Click here for more details on exemptions for not-for-profit organisations.

## 3. What principles should govern how we handle personal information and how are we ensuring that our policies and practices are compliant?

Whether or not you are required to register and pay the data protection fee, your organisaton's policies and practices must still comply with the six data protection principles.

- GDPR & Charitable Fundraising
- Th!nk Privacy Charity Sector Toolkit

**Data protection principles**
The six principles say that personal data much be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specific, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and up to date
5. Kept for no longer than necessary
6. Treated with appropriate security

**Lawful bases**
For personal information to be considered fairly and lawfully processed, you must meet at least one of the following:

- You have the consent of the individual for the processing
- You have a legal obligation to meet
- You need to process the information to meet a contract with the individual
- You need to process the information in order to protect life
- You are meeting a public task or exercising official authority
- You have a legitimate interest in the processing which is not overridden by the interests, rights or freedoms of the individual (in particular, where they are a child)

For more information about the lawful bases for processing, click here.

Source: www.diycommitteeguide.org

**Special category data**
Additional and separate conditions relate to the lawful processing of special category data (sensitive personal information).

Special category data is information relating to a person's:

Race or ethnicity
Political opinions
Religious beliefs
Trade union membership
Physical and mental health, and medical treatment
Sex life and sexual orientation

In addition, criminal offence data (relating to criminal convictions, allegations or proceedings) requires that one of these conditions defined in the Data Protection Act 2018 are satisfied.

For more information about conditions for processing special category data, click here and for criminal offence data, click here.

## Further guidance

Contact the Information Commissioner's Office in Northern Ireland for guidance on storage of personal information, legal requirements, rights of individuals, etc.

Tel: 028 9027 8757
Helpline: 0303 123 1114
Email: ni@ico.org.uk

Use NICVA's GDPR & Data Protection Toolkit

NICVA has produced a series of Data Protection Animation clips that explain GDPR in more detail. The topics covered are:

What is Personal Data?
Subject Access Requests
Personal Data Breaches
Consent & Legitimate Interests
Data Sharing

Visit Cyber Essentials for guidance on protecting your organisation against cyber threats.

Refer to the Fundraising Regulator guidance on data protection.

Charity Digital has guidance on Three Essential Strategies for Cyber Security.

Volunteer Now's Data Protection Policy is available here and NI Sports Forum Data Protection Policy is available here.

CRC's Information Security Policy is available here.

Source: www.diycommitteeguide.org