GENERAL DATA PROTECTION LEGISLATION: *WHAT CHARITIES NEED TO KNOW*

A TOOLKIT FROM DÓCHAS & FP LOGUE SOLICITORS

FPLOGUE

Dochas
The Irish Association of Non-Governmental Development Organisations

INTRODUCTION

This toolkit has been compiled by FP Logue Solicitors to give charities an overview of data protection and the General Data Protection Regulation.

This document contains a general summary and is not a complete or definitive statement of the law. Specific legal advice should be obtained where appropriate.

WHAT IS DATA PROTECTION?

Most charities and NGOs collect, use and keep "personal data" about people (such as members, donors, supporters, subscribers, employees, interns, volunteers) in digital form or in a filing system. If your organisation does this, and decides how and why the personal data will be processed, it is a "data controller" with obligations under data protection law.

Personal data is more than someone's name, address or date of birth. It means any information relating to an identified person or an identifiable person. This has broad scope and includes almost anything about or relating to a living individual.

Some personal data is "sensitive personal data", including information about a person's race, ethnic origin, political opinions, religious beliefs, trade union membership, physical health, mental health, sex life or sexual orientation. Additional legal requirements apply to sensitive data because this could be used in a more harmful way and is likely to be more private.

CURRENT LAW

As a data controller, your organisation must follow a number of principles to ensure that personal data is processed properly. These principles are binding and failure to observe them is in contravention of the Data Protection Acts. Additional conditions apply when processing sensitive data. The Data Protection Acts also grant rights to individuals. For example, an individual may request a copy of the personal data that you hold about them. The Data Protection Commissioner (www.dataprotection.ie) monitors and enforces compliance with data protection law. Currently, to ensure compliance, your organisation should have adequate policies relating to data protection, subject access requests, record retention and data security breach. Separately, your organisation should have an appropriate privacy notice, for example on its website, to ensure that individuals know what personal data your organisation collects and how it is used.

NEW LAW FROM 25 MAY 2018 – THE GDPR

The General Data Protection Regulation (GDPR) will come into force across the EU on 25 May 2018, replacing and repealing national data protection law. While the GDPR builds on existing data protection concepts, it introduces significant changes including legal and compliance obligations for data controllers and enhanced rights for individuals.

Under the GDPR there are six principles that must be followed when processing personal data:

1) lawfulness, fairness and transparency;
2) purpose limitation;
3) data minimisation;
4) accuracy;
5) storage limitation; and
6) integrity and confidentiality

Crucially, the GDPR introduces a new accountability principle on top of these requirements. This means that data controllers are not only responsible for GDPR compliance, they must be able to *demonstrate* compliance. This means record-keeping, policies, procedures and audits so that organisations can demonstrate their accountability and show this to the supervisory authority on request. There is an ongoing obligation to review this and update where necessary. The GDPR means that all data controllers will have to adopt a strategic, pro-active approach to how they collect, use and keep personal data and how they document these activities. This is likely to have significant resource implications for charities and NGOs.

Among other requirements being introduced by the GDPR are new or modified provisions about transparency, consent, security, data breaches, privacy notices, individuals' rights and complaints. In addition, supervisory authorities have extensive investigative, corrective and advisory powers, and they can impose significant fines on data controllers which must be "effective, proportionate and dissuasive". Individuals may also take legal action against data controllers, not just for compensation but for discrimination, reputational damage, loss of confidentiality, or other significant economic or social disadvantage.

PREPARING FOR THE GDPR

1) Awareness

The GDPR will be law in Ireland from 25 May 2018. Under the accountability principle not only must your organisation comply with the GDPR, you must also be able to demonstrate compliance.

- ⇨ Ensure that key people in your organisation know about the GDPR, how it is likely to impact your organisation, and the risks of non-compliance. Identify areas that could cause compliance problems.

2) Information you hold

Your organisation is likely to already have or be processing various amounts and types of personal data.

- ⇨ Identify the personal data you hold, why and on what basis you hold it, where it came from, how secure it is, and who it is shared with. You may need to carry out an information audit across your organisation or within particular units.

3) Communicating privacy information

Currently, when your organisation collects personal data you must give people certain information, such as your identity and how you intend to use and share their personal data. This is normally done by a privacy notice on your website. Under the GDPR there are additional things you need to tell people to ensure that processing activities are transparent, including the basis for processing the data, the data retention period, and that there is a right to complain. This must be in clear, understandable language.

- ⇨ Review your current privacy notice and put a plan in place for making necessary changes before the GDPR comes into force.

4) Individuals' rights

Individuals have enhanced rights under the GDPR, including to request a copy of their data, to correct inaccurate data, to have certain information erased, to object to direct marketing, to object to certain processing, to prevent profiling, data portability, and to complain to the supervisory authority.

- ⇨ Check your organisation's policies and procedures to ensure they cover all the rights individuals have, including how you would meet these obligations. Your privacy statement and consent forms will need to be reviewed and updated to take into account new rights.

5) Subject access requests

Individuals are entitled to see the personal data your organisation holds about them. Under the GDPR you have a month to comply with such requests and may no longer charge a fee.

When responding, you must give additional information. A request can only be refused if it is manifestly unfounded or excessive.

⇨ Update your organisation's procedures and plan how you will handle such requests within the new timescales and provide any additional information to the individual.

6) Basis for processing personal data

As well as complying with all the data protection principles, you need a legal basis for processing personal data, such as consent or a legitimate interest. Some individuals' rights will be modified depending on your basis for processing their data. You will also have to explain the legal basis for processing in your privacy notice and when answering a subject access request.

⇨ Identify the lawful basis for all of your data processing activities, document this and update your privacy notice to explain it.

7) Consent

The GDPR contains stringent conditions for obtaining consent as a basis for processing data. Consent must be freely given, specific, informed and unambiguous. Consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must be "explicit" for sensitive data. You must be able to demonstrate that consent was given. Prior to giving consent, individuals must be informed of their right to withdraw consent at any time and it must be easy for them to do so. For the first time, the GDPR provides additional safeguards for children accessing online services and consent will only be valid if it is given or authorised by a parent or guardian, and this must be verified.

⇨ Review how your organisation is seeking, obtaining and recording consent and whether any changes are needed, and ensure that you will have an effective audit trail.

8) Data breaches

You must have appropriate security measures in place in your organisation. Certain data breaches must be reported to the supervisory authority, without undue delay and where feasible within 72 hours. Any delay in notifying must be accompanied by a reasoned justification. You must keep internal records about data breaches. In higher-risk cases, affected individuals must also be notified.

- ⇨ Have appropriate training, procedures and a policy in place to prevent, detect, report, investigate and document a personal data breach.

9) Privacy Impact Assessments

Organisations engaged in data processing likely to result in high-risk to individuals' rights will be required to carry out a Privacy Impact Assessment and consult the supervisory authority to seek its opinion whether the processing is GDPR compliant. What "high-risk" means has yet to be clarified, but will include systematic and extensive evaluation of people (e.g. profiling) and large scale processing of sensitive data.

- ⇨ Review whether your organisation engages in high-risk data processing activities likely to significantly affect individuals and whether compulsory Privacy Impact Assessment applies.

10) Data Protection Officer

It will be mandatory for some organisations to appoint an independent Data Protection Officer ("DPO"). This applies to public authorities, public bodies (except courts) and organisations whose core activities involve regular and systematic monitoring of people on a large scale or consist of processing on a large scale of special categories of data. The role of a DPO is specifically described in the GDPR.

- ⇨ Review whether your organisation is required to designate a DPO and, if so, assess whether your current approach to data protection compliance will meet the GDPR's requirements.

11) Data processing contracts

For the first time the GDPR imposes obligations and liability on "data processors" (they carry out data processing on behalf of a data controller). If you use an external or outsourced data processor you must ensure they too are in compliance with the GDPR.

- ⇨ Contracts with any data processors must be reviewed to ensure they meet the GDPR's requirements and clearly specify the scope of the data processor's responsibilities.

NOTE

This document contains a general summary and is not a complete or definitive statement of the law. Specific legal advice should be obtained where appropriate.

FP LOGUE SOLICITORS

For expert legal help with data protection, contact FP Logue Solicitors

Niall Rooney
FP Logue Solicitors
Tel: 01 531 3510
Email: info@fplogue.com
Web: www.fplogue.com

DÓCHAS

Dóchas is the Irish Association of Non-Governmental Development Organisations.

By joining Dóchas you can **connect and collaborate** with like-minded organisations, strengthen your **knowledge and expertise**, and **influence key decision-makers** at national, European and global levels. Through Dóchas, you can build your skills, add value to your work and that of the sector and help shape the direction of global development by sharing practical knowledge and resources.

If your organisation is interested in Dóchas membership, you can download application forms on our website: http://dochas.ie/membership/options