DATA PROTECTION & THE GDPR – WHAT CHARITIES NEED TO KNOW

What is data protection?

Most not-for-profits, charities and voluntary organisations collect, store or process "personal data" about people (such as employees, members, service users, supporters, donors, subscribers) in digital form or in a structured filing system. If your organisation does this, and it controls and is responsible for the personal data which it holds, it is a "data controller" with legal obligations under the Data Protection Acts.

Personal data is more than a name, address and contact details. It means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. This has broad scope and includes almost anything relating to a living person.

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

Current law

If your organisation is a data controller, it must follow a number of fundamental principles to ensure that personal data is processed properly:

1) Obtain and process information fairly and lawfully;
2) Keep it only for one or more specified and lawful purposes;
3) Use and disclose it only in ways compatible with these purposes;
4) Keep it safe and secure;
5) Keep it accurate, complete and up-to-date;
6) Ensure that it is adequate, relevant and not excessive;
7) Retain it no longer than is necessary for the specified purpose or purposes for which it was obtained;
8) Give a copy of personal data to an individual, on request.

These principles are binding on data controllers and failure to observe them is in contravention of the Data Protection Acts.

Additional conditions apply when processing sensitive personal data, which usually requires the individual's explicit consent to the data processing.

The Data Protection Acts also grant certain rights to individuals, who are known as "data subjects". For example, a data subject has the right to ask for a copy of personal data you hold about him/her.

The Data Protection Commissioner (www.dataprotection.ie) monitors and enforces compliance with data protection law in Ireland.

Currently, to ensure compliance, your organisation should have policies and procedures in place relating to data protection, data subject access requests, record retention and data security breach.

Separately, your organisation should have appropriate notices, for example on its website, to ensure that individuals are made aware of 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 national data protection law. The GDPR builds on existing familiar data protection concepts and rules, however there are new elements and significant enhancements.

Under the GDPR there are six general principles to 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 will not only be responsible for compliance with the GDPR, but they must also be able to *demonstrate* compliance. This means record-keeping, documentation, policies, procedures and audits so that organisations who are data controllers can demonstrate accountability and show this to the supervisory authority on request. There is an ongoing obligation to review this and update where necessary. All data controllers will have to adopt a strategic, pro-active approach to how they process and handle personal data. This will have significant resource implications for not-for-profits, charities and voluntary organisations.

Among other requirements introduced by the GDPR are new or modified provisions about consent, data breaches, transparency, privacy notices, individuals' rights, and the appointment of data protection officers. In addition, there are severe financial penalties for non-compliance. Depending on the category of infringement, administrative fines may range from (i) up to €10 million or up to 2% of global annual turnover, whichever is higher, or (ii) up to €20 million or up to 4% of global annual turnover, whichever is higher.

Preparing for the GDPR

1) Awareness

   From 25 May 2018, the GDPR will be directly applicable in Ireland without the need for implementing legislation. Under the new accountability principle not only must your organisation comply with the GDPR, you must also be able to demonstrate compliance.

   ⇨ Ensure key people in your organisation know about this, how it will impact your organisation, and the risks involved in non-compliance. Identify the areas that could cause your organisation compliance problems. Consider designating a privacy champion in your organisation to take a lead on data protection knowledge and compliance issues.

2) Information you hold

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

   ⇨ Document the personal data you hold, where it came from and who it is shared with. Consider carrying 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 the organisation's website. Under the GDPR there are additional things you need to tell people to ensure that processing activities are transparent, including the legal basis for processing the data, the data retention period, and that there is right to complain. Your organisation will have to explain the basis for processing personal data in its privacy notices. All of this needs to be in clear and easily understandable language.

   ⇨ Review your privacy notices and put in place a plan for making necessary changes before the GDPR comes into force. All privacy notices and policies will need to be reviewed and revised to comply with the additional information requirements and to ensure that processing is fair and transparent.

4) Individuals' rights

Individuals have enhanced rights under the GDPR including data subject access, to correct inaccurate data, to have their information erased, to object to direct marketing, to prevent automated decision-making and profiling, and data portability (receive personal data electronically in a common format for transfer to another organisation).

⇨ Check your organisation's procedures to ensure that they cover all the rights individuals have, including how you would meet these obligations, and how you would delete personal data or provide data electronically and in a commonly used format. Your privacy statements and any other 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 will have a month to comply with such requests, rather than the current 40 days. You may no longer charge a fee for dealing with requests. When responding, you must give information about, for example, your data retention period, the right to correct inaccurate data and the right to complain to the supervisory authority. A request can only be refused if it is manifestly unfounded or excessive.

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

6) Basis for processing personal data

Under current law your organisation's basis for processing personal data does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your basis for processing their personal data. You will also have to explain the basis for processing personal data in your privacy notice and when answering a subject access request.

⇨ Review the types of data processing you carry out, identify the basis for carrying it out, and document it to help you comply with the new accountability requirement.

7) Consent

The GDPR contains more stringent conditions about obtaining consent from individuals. Consent will become more difficult to rely on in order to legitimate processing of data. This is particularly relevant for organisations involved in direct marketing, promotional or fundraising activities. Consent must be freely given, specific, informed and unambiguous. Consent cannot be inferred from silence, preticked boxes or inactivity. Consent must be "explicit" for sensitive data. Your organisation 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 special safeguards for children in the context of consent given online by a child. Consent will only be valid if it is either given or authorised by the child's legal guardian. You must make reasonable efforts to verify that consent was in fact given by the child's legal guardian. If collecting children's data your privacy notice must be written in language that children will understand.

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

⇨ If applicable, identify any children whose data your organisation processes, identify the conditions legitimising processing, and put systems in place to verify ages and obtain parental/guardian consent.

8) Data Breaches

The GDPR requires all organisations to have appropriate security measures in place and introduces a new mandatory obligation to report data breaches to the supervisory authority without undue delay and where feasible within 72 hours of becoming aware of it. Any delay in making a notification must be accompanied by a reasoned justification. Your organisation must keep an internal record of all data breaches. In some cases, the affected individuals must also be notified.

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

9) Privacy Impact Assessments

Organisations engaged in data processing which is likely to result in high-risk to rights of individuals will be required to carry out a Privacy Impact Assessment and consult the supervisory authority to seek its opinion whether the processing operation complies with the GDPR. What "high-risk" means has yet to be fully clarified, but it will include systematic and extensive evaluation of individuals (including 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"). The organisations subject to this requirement are public authorities and public bodies (except courts) and organisations whose core activities involve the regular and systematic monitoring of data subjects 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 you are 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" (organisations whose main data-related activity is providing services to other entities). If you use the services of an external data processor you must ensure they too are in compliance with the GDPR.

⇨ Any contracts with data processors should be reviewed to ensure they meet the GDPR's requirements and clearly specify the scope of the data processor's responsibilities.

More information

Contact us with any questions.

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

11/04/2017
