General Data Protection Regulation (GDPR)

Some helpful information for small groups and associations.

Background

The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years. It comes into force on May 25th, 2018. The EU General Data Protection Regulation (GDPR) was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.

Aims

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world.

Who does the GDPR affect?

The GDPR not only applies to organisations located within the EU but it will also apply to organisations located outside of the EU (under specific circumstances).

What constitutes personal data?

Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

Data Controller

A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the Data Processor is a person or an entity which processes personal data on behalf of the Data Controller.

Consent

The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and use clear and plain language. It must be as easy to withdraw consent as it is to give it. Sanctions and fines are significant and cannot be ignored.

Extracts from: *https://www.eugdpr.org/*

So what can I do?

Data Protection has always been there and enforced through the Data Protection Act 1988 and 2003. If you hold data on individuals, you are responsible for the safe use of that data and can only use that data for the purpose(s) it was given. As an example; if you asked a person to give you their email or address so that you can send them a brochure on your group, you cannot use that

information to send them details about your fundraising events. It is also important to know that every individual has the right to email or write to you for a copy of the data you hold on them.

Here are some simple steps that will help your group or association.

- Appoint a person within your group to take ownership of the data you hold.
- If you have a database that you use to communicate with people, make sure that you have their written consent to do so.
- If you are concerned that you do not have written consent for data that you hold, update your files by seeking written consent from the individual(s) in question.
- You can only keep data for only one or more clearly stated and lawful purposes.
- Make sure that the information is factually correct, complete and up-to-date.
- If you issue membership Forms, ensure there is a section that covers Data Consent and gives you the written permission of the member to communicate with them on matters they have chosen to be communicated with.
- Ensure the data you have is securely stored in a safe location and that access is restricted.
- Do not share any data with Third Parties unless required by law e.g. An Garda Siochána.
- If you have a website, make sure you have a Privacy Statement on it.
- If you use Attendance Sheets at events to gather personal information such as names, emails and mobile numbers, you must inform each attendee that you are gathering this information, why you need it and how you intend to use it.
- If you send emails to more than one person at a time (unless to members of the Executive Committee), ensure that you send the email to yourself as the “recipient” and that all other addresses are shown in the “Bcc” section. This way, the other addresses are protected.
- If you are asked to remove /delete data from your database, you have 40 days to do so.
- Put data breach prevention systems and notification systems in place such as locks and CCTV, authorisation levels, password protection and back-ups.
- Invest in basic training so to understand the basic requirements for holding data.
- Communicate with the Office of the Data Protection Commissioner immediately, and the Data Subject, where necessary, if a breach occurs.