General Data Protection Regulation – GDPR
Guidance for Community Alert Groups and Community Councils

Introduction

You have probably heard of GDPR, the new General Data Protection Regulations, which come into effect on 25th May. This is an initial guidance document to get you started. It is aimed at typical groups who maintain simple personal data (eg Text Alert databases). Groups who maintain more complex personal data may need further guidance. GDPR has extensive obligations and potential penalties. However, much of it is common sense. If you have reasonable policies and procedures, preferably written, in place, you are probably well on the way to being compliant, but now is a good time to review these.

Does this apply to my group?

If you keep personal data you are a Data Controller, and this applies to you. Personal data includes names, addresses, and/or mobile phone numbers. It can be computerized or manual (eg paper). If you keep "sensitive data" (eg racial origins, physical or mental health) further obligations arise. If you process data (eg send out SMS messages yourself) you may also be a "Data Processor" (you can be both). The greater requirements are for Data Controllers.

What are my obligations as a Data Controller?

The regulations state that you must:

- **Obtain and process information fairly**
- **Keep it only for one or more specified, explicit and lawful purposes**
- **Use and disclose it only in ways compatible with these purposes**
- **Keep it safe and secure**
- **Keep it accurate, complete and up-to-date**
- **Ensure that it is adequate, relevant and not excessive**
- **Retain it for no longer than is necessary for the purpose or purposes**
- **Give a copy of his/her personal data to an individual, on request**

Further information on these obligations is available at https://www.dataprotection.ie/docs/A-Guide-for-Data-Contollers/y/696.htm.

What do I need to do?

There are a number of steps you should carry out initially. These include:

1. Review and document what data you hold, and whether you need to hold it. For example, most groups using Text Alert will hold names, addresses, telephone numbers, and payment details. If you hold more than this you should consider if this is necessary.
2. Ensure you have consent. This should be written consent which specifies how the data will be used. For example, a simple sign up form from an individual giving their consent to using their telephone number to issue Text Alerts could be used. A sample template is available from your Community Alert Development Officer. If you

have gathered data without this explicit consent you should obtain the documentation now (eg get forms signed as part of renewal).

3. Allow subscribers to withdraw their consent and have a policy for this. This can be quite simple and might say that once you receive written instructions from a subscriber you will delete or destroy their details within, say, one month.
4. Secure access to personal data. Physical data (eg forms) should be controlled by a specified individual in your group and physically secured (eg a locked filing cabinet). Electronic data (eg spreadsheets) is more complex but, for example, should be stored on a nominated device (eg one computer). This device should be secure and should be fully backed up. The minimum security is a password and devices should also be physically secured. For a desktop, this might mean limited physical access; laptops should be encrypted. The device should be properly maintained (eg all operating patches applied promptly).
5. Nominate one person from your group to be responsible for this data.
6. Consider whether you might have further obligations. For example, if you use mailing lists, there are further obligations.

What are data security breaches?

A data security breach occurs if the personal data you store is compromised; for example if it potentially becomes available to unauthorized third parties. Examples would include losing a device on which the data is stored (eg losing a laptop). Such breaches may need to be notified to the Data Protection Commissioner, and the affected persons, within 48 hours.

This is when your procedures may be scrutinized, so it is important the policies and procedures be in place before any breach occurs. Further information on disclosure requirements is available at https://www.dataprotection.ie/docs/Data-Security-Breach-Code-of-Practice/y/1082.htm.

Direct marketing

If you use text or email to contact individuals with direct marketing, then you must:

- Have their explicit consent and be able to prove it (eg a written form, or use of a subscriber service such as MailChimp which records IP addresses).
- Allow them to opt out at any stage, and easily (eg an "unsubscribe" option on an email, which takes effect immediately and without complication).
- Other requirements can be found at https://www.dataprotection.ie/docs/DIRECT-MARKETING-A-GENERAL-GUIDE-FOR-DATA-CONTROLLERS/y/905.htm.