Campaign for Better Transport

GDPR: Guidance for local groups

Introduction

The General Data Protection Regulations are an EU law that comes into effect in the UK on 25 May 2018. It replaces the Data Protection Act and introduces some new requirements, and a new fines regime, for all organisations who handle personal data, regardless of sector or size. There has been a lot of publicity around the new regulations, mostly because the sizes of the possible fines are huge, but the meat of the regulations is not actually vastly different from the existing Data Protection Act. This is a good opportunity to review your data protection policies and practices, but there's no need to panic!

Principles

Personal data has a wider definition under the new Regulations. Any information that can be used to identify an individual is now personal information: for example name, address, email addresses or an identification number you have applied if that can easily be traced to an individual within your systems.

There are a few simple principles you need to follow when processing personal data.

- **Consent:** You should aim to get clear and unambiguous consent from each person you wish to hold data for; collected when you collect the data. You should have a clear privacy policy that outlines what you will do with the data, how you will store it, keep it secure and delete it.

- **Data security**: You must protect people's data where you store it. If you have spreadsheets on local computer hard drives you should consider password protecting them. Physical lists should be kept in locked cabinets. If you use tools such as Mailchimp or cloud storage you should use secure passwords and restrict who has access to the accounts.

- **Right to opt out**. Individuals retain the right to opt out from communications from you at any time so you must let people know how they can do this regularly and respect their wishes. Individuals can also request to see all the information you hold about them so you should consider how you would meet this request if it is made.

What should we do now?

In order to prepare for the new Regulations you should:

1. **Data review:** Work out what data you hold on people, and where you're getting that data from. Review what consent you have from people to hold this data and consider whether this needs updating. Also think about where this data is stored, who has access and whether this is secure

2. **Policy review:** Have a look at your privacy policy, or put one in place if you don't have one. Think about where people can view the policy, what it should say and how you would deal with a subject access request or a request for information to be deleted.

3. **Training:** Make sure all staff or volunteers who are involved with your organisation are clear about your data processes.

Frequently asked questions

Do I need to ask all of the people on my mailing list to 'opt in'?

No. There's been a lot of controversy about this, and many organisations have chosen to exceed the required standard by asking people to opt back in to mailings but there is no requirement to do so. You must have either consent or legitimate interest to contact people, and you must offer them a chance to opt out at regular intervals but it's not required to move to an opt in only model. Legitimate interest is assessed by a three-part test:

- **Purpose test** – is there a legitimate interest behind the processing?
- **Necessity test** – is the processing necessary for that purpose?
- **Balancing test** – is the legitimate interest overridden by the individual's interests, rights or freedoms?

The definition is not tightly set out in the Regulations so in general it would be more prudent to rely on explicit consent for mailing lists and similar communications.

Is it OK to keep a spreadsheet of all my members' or supporters' information?

This is OK as long as the information is secure. So you may consider password protecting your Excel Spreadsheet, and should make sure you're not sending un-protected data to other people over email.

Can I share my member lists with other people?

Not unless you have explicit consent. There are a specific set of rules you need to follow if you are sharing data with other organisations; you should consider seeking legal advice before you do this.

Do I need to register with the Information Commissioner?

Probably not. Most organisations who are processing personal data do need to register with the Information Commissioner, but there are exemptions for small non-profit organisations. You can use the self-assessment tool on the ICO website to check if you need to to do: https://ico.org.uk/for-organisations/register/self-assessment/

Where can I find more information about GDPR?

ICO guidance:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Friends of the Earth guidance for local groups:
https://friendsoftheearth.uk/local-groups/gdpr-guidance

White Fuse Media guidance for small charities
https://whitefusemedia.com/blog/gdpr-small-charities

Charity Finance Group more details guidance:
http://www.cfg.org.uk/resources/Publications/~/media/Files/Resources/CFDG%20Publications/CFG266_GDPR.pdf

Sample privacy policy: White Fuse Media have produced a guide for you to download:
https://whitefusemedia.com/blog/data-protection-policy-template-charities

Appendix

Data mapping exercise

To carry out a data mapping exercise you could try making a spreadsheet, analysing all the places you collect data by asking the following questions. You should have a new column for each different source of data you collect.

Data collection point	***EXAMPLE*** ***Mailing list***
What data is collected?	*Name, email address, postcode*
What consent is obtained?	*On the signup form*
Where is this data stored?	*In Mailchimp*
What is the data used for?	*To send monthly updates about our campaigns*
Who can access the data?	*Communications team*
Is the data shared externally?	*Stored in Mailchimp*

When is the data reviewed?	*Never*
How long is the data kept?	*As long as people remained signed up to the list*
When is the data deleted?	*When people elect to opt out*