INFORMATION SHEET 3.9

DATA PROTECTION

An Independent Charity No. 1075060

This information sheet provides a brief overview of the main requirements of data protection legislation and its implications for voluntary and community groups. New data protection standards were introduced by the European Union under the General Data Protection Regulation (GDPR) and this was enshrined in UK law by the Data Protection Act 2018.

WHAT IS COVERED BY DATA PROTECTION LEGISLATION AND DOES IT APPLY TO US?

Data Protection is all about handling personal information responsibly and taking steps to ensure it is secure and not misused. Your organisation is almost certainly covered by the legislation, even if all you do is keep a list of members' contact details.

The data covered are any personal information in any format. This could include paper files, such as membership forms, attendance sheets, diaries and minutes of meetings, and also personal details that are stored electronically, such as on a computer. It also covers other information, including photos, CCTV footage or other images, the IP addresses of people visiting your website and e-mails. The legislation covers the processing of data from collection to storage, usage, how it is organising, updating and amending, sharing and finally destroying the data.

The EU GDPR is an EU Regulation and it no longer applies to the UK. If you operate inside the UK, you need to comply with the Data Protection Act 2018 (DPA 2018).

The provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. In practice, there is little change to the core data protection principles, rights and obligations. GDPR recitals add depth and help to explain the binding articles. Recitals continue to have the same status as before – they are not legally binding; they are useful for understanding the meaning of the articles.

The EU GDPR may still apply to you if you operate in the EEA, offer goods or services to individuals in the EEA, or monitor the behaviour of individuals in the EEA.

There are six Guiding Principles, which should be adhered to when processing personal data to ensure fairness:

1. Lawfulness, fairness and transparency
   - Data should be processed lawfully, fairly and in a transparent manner.
2. Purpose limitation
   - Data should only be collected for specific, explicit and legitimate purposes.
3. Data minimisation
   - Data should be adequate, relevant and limited to what is necessary.
4. Accuracy
   - Data should be accurate and, where necessary, kept up to date.
5. Storage limitation
   - Data should be kept only for as long as is necessary.
6. Integrity and confidentiality.
   - Data should be processed in such a way as to ensure the integrity of the data and the confidentiality of the data subjects.

GLOSSARY OF KEY TERMS:

Data Controller: Any person or organisation that decides what personal data to collect and how to process it.

Data Subject: Any living person about whom you collect, hold or use personal information.

Data Processing: From the moment you take someone's details to the moment you shred or delete their file, you are processing data about them.

Continued...

INFORMATION SHEET 3.9

DATA PROTECTION

An Independent Charity No. 1075060

Data Processor: Any person or organisation that processes data on behalf of another but not employees of the Data Controller.

Personal Data: Any information relating to a living person who can be directly or indirectly identified because of the information.

WHAT ARE THE PRACTICAL IMPLICATIONS?

The data isn't yours! The data that you collect about your members or beneficiaries isn't yours: it's theirs, and they can instruct you to stop processing their data, insist that you correct any errors and generally decide what you may or may not do with their data.

Better communication: You need to tell people why you are collecting their data and what you intend to do with it. You should tell them this at the point of collecting the data by giving them a Privacy Notice or access to a notice such as on your website.

You will probably need consent: You may well need signed consent before you process personal data, but there are five other legitimate reasons why you may process data, depending on the circumstances, including to enter into a contract, to meet a legal obligation, to protect the vital interests of a subject, to perform a task that is in the public interest and to pursue a legitimate interest.

Responding to a subject access request: If someone asks for all the information you hold on them then you must provide it within a month and at no charge. Only in exceptional circumstances can you ask for more time and, even then, you are limited to two months.

Dealing with a data processor: If you ask another person or organisation to process data on your behalf, e.g. to evaluate a project or provide statistics, then you need to enter into a formal contract that specifies the obligations of both parties.

Data retention: Your privacy notice and data protection policy should specify how long you intend to retain data.

Privacy by design and default: When starting a new project data protection should be one of the first topics you consider. Think about the security measures you must put in place to protect the data.

Children: Young people under 13 years of age must be given special consideration particularly in relation to obtaining consent.

Data breaches: A breach of security leading to the destruction, loss, alteration, unauthorised or accidental disclosure of, and access to, personal data may need to be reported to the Information Commissioner's Office.

RELATED DOCUMENTS

3.1 Effective Meetings
3.2 Running an AGM
3.3 Preparing your Annual Report
3.4 Organising a Community Event
3.5 Writing a Business Plan
3.6 Employing a Worker
3.7 Disclosure and Barring System
3.8 Quality Assurance
3.9 Data Protection
3.10 Closing your Organisation

North Tyneside VODA, Spirit of North Tyneside Wing, 2nd Floor, Wallsend Customer First Centre, 16 The Forum, Wallsend, NE28 8JR
Tel 0191 643 2626, www.voda.org.uk, Charity number 1075060