Toolkit Guidance Note: The General Data Protection Regulation (May 2018)

The General Data Protection Regulation or GDPR comes into force on 25 May 2018. That's not new news. *But it is a fact.*

It replaces the Data Protection Act of 1998, and in many ways strengthens the rights of individuals in respect of their personal data, and how it is stored and used.

It will affect all sectors of the population, including business and charities.

This information guide seeks to provide community organisations with some basic help and information on the subject, including an explanation of some of the key terms you are likely to come across. It is not short or concise, as there is some complexity contained within the GDPR and its implications. In addition, guidance is still being prepared on this subject by the Information Commissioners Office (or ICO) so organisations should seek as much information on the subject area as they possibly can, from whatever source, between now and May 2018.

Useful Resources are shown at the rear of this note.

Let's start by exploding two simple myths:

The biggest threat to organisations from the GDPR is massive fines.

Fact:

This law is not about fines. Although some large charities have been fined recently, the reasons are more to do with selling or swapping data rather than data management. The ICO role is to advise and guide, and not to punish. That being said, every organisation (whether large or small) that handles personal data should prepare themselves for the GDPR. Fore-warned is fore-armed.

The GDPR is an unnecessary burden on organisations.

Fact:

The new regime is seen as an evolution in data protection, not a revolution. Most reliable commentators argue that if you already have robust data protection principles in place, the GDPR will not be overwhelming.

Let's explain some Key Terms as simply as possible:

This is not easy, as terms can often be complex and detailed.

Consent:

The GDPR is raising the bar to a higher standard for consent. Consent under the current data protection law has always required a clear, affirmative action: The GDPR clarifies that pre-ticked opt-in boxes are not indications of valid consent. The GDPR is also explicit that you've got to make it easy for people to exercise their right to withdraw consent. The requirement for clear and plain language when explaining consent is now strongly emphasised: You also have to make sure that the consent you have already obtained meets the standards of the GDPR. If not, you will have to refresh it. There are a number of other ways in which data can be processed without consent but most community based organisations will probably want or need consent, and therefore understanding what consent is and how you obtain it is crucial.

Personal Data Definition:

Personal data will mean any information relating to an identified or identifiable natural person. This will include unique identifiers such as people's IP addresses and cookies (where they are used to uniquely identify their device for example). This makes cookie use subject to the same consent requirements as any other.

Right to Access:

The person whose data you are collecting has the right to obtain confirmation of whether personal data concerning them is being processed, where it is being processed, and for what purposes. This must be provided free of charge unless the request is seen as repetitive, excessive or unfounded.

Right to be Forgotten:

The data subject can insist that the controller (the organisation collecting the information) erase all personal data about them and stop the processing of it by third parties.

Breach Notification :

Any breach of the GDPR must be sent to the Information Commissioners Office, and must be sent within 72 hours of becoming aware of the breach. The data subject must also be notified without undue delay if it is likely to result in any risk to their rights and freedoms.

Privacy by Design:

Data controllers (organisations which collect personal data) must implement appropriate technical and organisational measures to meet the GDPR requirements; they must hold and

process data that is absolutely necessary for the completion of their duties, and limit access to personal data to those doing the processing.

Data Portability:

The new regulation will give individuals the right to transfer their data from one controller to another. So organisations, on request, must be able to deliver a person's data in a suitable format. Data collected via online surveys is immediately compliant with the data portability rule as it can be provided instantly without needing any further handling.

Data Controllers:

Some larger organisations will appoint a member of staff as a Data Controller (someone who has been trained and developed to manage the compliance function). This is simply not possible for smaller community based organisations. In this case, a basic awareness of data consent and processing is required amongst all staff and volunteers.

Lawful Processing:

For processing to be lawful under the GDPR, you need to identify a lawful basis before you begin. These are often referred to as the "conditions for processing" under the current Data Protection Act. It is important that you determine your lawful basis for processing personal data and document this. This becomes more of an issue under the GDPR because your lawful basis for processing has an effect on individuals' rights. For example, if you rely on someone's consent to process their data, they will generally have stronger rights in law.

Where do we start?

A good starting point is to examine the ICO's guidance – and their 12 step model to being prepared for the GDPR. Pay particular attention to the following points:

The Information you hold:

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas.

The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles by having effective policies and procedures in place.

Communicating privacy information:

You should review your current privacy notices and put a plan in place for making any necessary changes in time for the GDPR implementation. When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data and your data retention periods.

Individuals' rights:

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format. The GDPR includes the following rights for individuals:

The right to be informed
The right of access
The right to rectification
The right to erasure
The right to restrict processing
The right to data portability
The right to object
The right not to be subject to automated decision-making including profiling.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the current Data Protection Act but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? And who will make the decisions about deletion. Ensure that this is clarified in advance of May 2018.

Lawful basis for processing personal data:

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the current act. It should be possible to

review the types of processing activities you carry out and to identify your lawful basis for doing so. You should document your lawful bases in order to prepare for the GDPR.

Consent:

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard. You should read the detailed guidance the ICO has published on consent under the GDPR, and use our consent checklist to review your practices. Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Public authorities and employers will need to take particular care. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data. You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

Children:

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services ('information society services') to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'. This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent has to be verifiable, and that when collecting children's data your privacy notice must be written in language that children will understand.

Further Resources:

ICO: The 12 Step Model for preparation:

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

ICO: What to expect and when:

https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/

Trustee: Preparing for the General Data Protection Regulation:

https://iapp.org/media/pdf/resource_center/TRUSTe_GDPR_Report_FINAL.pdf

Support Cambridgeshire: Welcome to the GDPR:

https://www.supportcambridgeshire.org.uk/welcome-gdpr-whats/

Hunts Forum: Important Impacts of the GDPR:

http://www.huntsforum.org.uk/images/pdf/gdpr.pdf

GDPR Associates: What is GDPR?

https://www.gdpr.associates/what-is-gdpr/

Bates, Wells and Braithwaite: 10 Top Tips for GDPR:

http://www.bwbllp.com/knowledge/updates/2017/05/25/gdpr-one-year-to-go/