GDPR for Committees and Staff Members of Charities and Community Groups

GDPR is the new buzz word – due to take effect from 25th May 2018. GDPR means General Data Protection Regulations. It is new UK law, derived from EU law, and updates the regulations under the Data Protection Act 1998 (DPA).

In most aspects if your organisation was fully compliant with the regulations under the DPA then little more will be needed. But you will need to review and assess compliance, even if yours is a very small organisation.

The reason behind introducing the new regulations is because the way personal data is processed has changed dramatically over the last 20 years. Technological change is the biggest change but also there are changes in the way data is used for commercial purposes, for charitable fund raising and for data coordination and sharing.

The Eight Data Protection Principles remain at the heart of the regulations

data must be:

1. Fairly and lawfully processed;
2. Processed for limited purposes;
3. Adequate, relevant and not excessive;
4. Accurate;
5. Not kept for longer than necessary;
6. Processed in line with your rights;
7. Secure, and;
8. Not transferred to countries without adequate protection;

GDPR makes “Privacy by design” an express legal requirement. Therefore any charity or community group that records people’s name and any more information must consider the Data Protection requirements.

Summary simple rules for simple situations

The committee of any group that has computer records or even paper records of their members or beneficiaries are legally obliged to consider why they keep the data, that it only be used with consent of the person in the way(s) agreed and that it is kept secure and private. Committees of community groups and charities must get help if they do not know what to do to meet the GDPR requirements. There are legal justifications for processing data; the group needs to determine which applies to them. See appendix

- Personal data must always be processed fairly, handled for intended purpose and only in ways that an individual would reasonably expect. Obtain and keep record of consent
- Don’t download data to laptops or pen drives without password encryption
- Don’t send data files by email unless absolutely necessary
- Maintain confidentiality on need to know basis
- Train all staff, including volunteers, and obtain confidentiality agreement
- Delete or destroy securely when no longer required

Some Definitions

Personal Information is data about any living person. This applies to paper records and those on computers. It would include computer IP addresses and internet cookies.

Sensitive Personal Information (under GDPR called Special Categories) would include data about:

- Race or ethnic origin
- Political opinions
- Religious or similar beliefs
- Being a member of a trade union
- About the physical or mental health
- About sexual life
- About offences
- This also includes biometric and genetic data such as DNA or fingerprints

The Data Controller is the organisation (or person) who decided the purposes for which and the manner in which any personal data are, or are to be, processed.

The term **"Data Processing"** is central to everyone's understanding of the subject. It includes anything done with data including the fact that it remains on a computer without anyone accessing it. It refers to deleting it. It includes everything about how it is accessed, changed or compiled. The data processor is the organisation or person undertaking the processing. It may be a contractor on behalf of the data controller. There must be a formal contract between the Data Controller and any external Data Processors

Data Subject is the term referring to the person whose information / data is held.

Subject Access is the provision for the person to be provided with all the information about themselves.

Breaches of data must be reported to the UK regulator – the Information Commissioners Office (ICO). It must also be reported to the Charity Commission as a serious incident.

Note that under GDPR, the ICO has power to issue higher fines. This is up to €20m or 4% of turnover.

Organisational Data is not subject to DPA or GDPR as it is not in relation to a living person. So the contacts at an organisation using the organisations domain is not personal data. For example manager@greatgroup.org.uk is not personal but Fred.Smith@greatgroup.org.uk may be. However many community groups are so small that their contact details would be the same as their personal contact details and so DPA and GDPR will inevitably apply to virtually all community groups.

For Charities and Community Groups

1. You must design your DP policy and procedure to suit the data processing requirements of the organisation. Therefore your board of trustees or Committee must have examined the requirements of GDPR and have taken a decision in how they will process personal data. The way this would be seen is if there is a Data Protection policy.
2. It may be necessary to pay the DP fee to the ICO. (same as registration or notification)
3. People must give consent to their data being processed. The consent must be clear, recorded and be able to be withdrawn. Data Controllers must be able to demonstrate that they have been given consent.
4. People have the right to have all their data removed; this is called 'the right to be forgotten'.
5. If people's data is given to another organisation, eg Payroll or Pensions or other service, then there must be a binding contract between the data controller and the contracting processor.
6. Staff, employees and volunteers, will need training. It will be necessary for them to declare compliance with policy. This would normally be by signing a Confidentiality and Data Protection Agreement.

Complying with Good Practice

- Have a Data Protection Policy that has been updated for GDPR.
- Undertake a Data Protection audit to identify extent and use of personal data
- Data security policy and procedures that enable data to be kept securely and safe. Therefore firewalls, anti-virus and passwords must be good. Data must be kept up to date and regularly backed-up.
- Evidence of data subject consent to handling data. For employees this will include passing of relevant information to contractors for payroll, pensions and other employment processes.
- Evidence of training for all staff who handle data, including any more than knowing the name of someone in the charity. (unrecorded personal conversations are not included).
- Evidence of staff agreement of understanding and to comply with the policy and procedures.
- Data can be processed if there is "legitimate interests" – such as holding employee or membership information.
- Data can be shared if it is in the "Vital Interests" of the person – such as with a hospital emergency department after an accident.

Data Protection Officer

A Data Protection Officer (DPO) must be appointed in certain circumstances. This is for public organisations like councils or the NHS, or when there are data subjects who are monitored on a large scale or when a large amount of sensitive personal data is handled –sensitive data would include any criminal records information. The DPO must be a senior person reporting at the highest level. They must have independence to undertake their audit responsibilities.

Most small charities and community groups would not have to appoint a DPO. However the committee may wish to appoint a lead person who is well trained in Data Protection and GDPR. Committees that are unsure about GDPR must (according to the Charities Commission) ask for help. Help is available from Community Action Fareham.

The fines for non-compliance are now much higher. That said, ICO says it will help rather than fine. Two new offences under GDPR include re-identifying individuals from anonymised data and altering personal data to prevent disclosure such as after a Subject Access Request (SAR)

Fundraising

Using databases of supporters, donors and members for fundraising purposes requires special consideration under the regulations. Consent to the charity holding the information, consent to be sent fundraising communications in specific ways and the right to change or cease must be included.

It has been and will continue to be an offence to manipulate data and share data. RSPCA and BHF were fined £43,000 in 2016 and 11 more in 2017 were fined a total of £138,000. They had been carrying out processing contrary to Data Protection Act regulations including:

- "wealth screening" – identifying people from various sources according to their wealth
- obtaining data from other sources to add to their own data bases – "data matching"
- and sharing the data with other charities without the donor's consent.

This illustrates that the collection and use of data must be transparent and only used for the declared purposes.

If you use personal data for fundraising and your costs of fundraising are over £100k per year you are expected to register and pay a levy. Guidance about fundraising is on the regulator's website www.fundraisingregulator.org.uk

Email newsletters and campaigns

People must only be sent email newsletters or promotions to their personal addresses if they have specifically signed up to receiving information from you. They have a right to be removed effectively from your list, and "to be forgotten". It is expected practice that all emails will provide the "From" address, the organisations details and an option to be removed from the mailing list.

If organisations have email lists without a record of consent to join it then, for personal email addresses, the consent must be renewed. If there is no response it's a no!

Emails sent to lists of people must always be sent blind copied unless you have express permission to show the distribution – eg for a committee or internal at work.

Data Protection & Privacy Statement

All forms that collect people's name and information, for either an ongoing membership purpose or a one off event record must have a Data Protection Statement. There should also be a tick for consent to process the data – that would include keeping the paper form and transferring the data to a computer as well as any other ongoing use. The statement must say how the data will be used, to add to an email distribution list or to share the data. The consent must be clearly given for the specific purposes.

Privacy notes may be separate and have more detailed content.

Example / Model statement

The information given will be added to a computer system for the purposes of maintaining our membership administration. Please tick the boxes below to give your consent to how we will communicate with you and use your personal information.

☐ *I give consent to my information being kept on [organisation]'s systems for administration of membership*

☐ *I give consent to receive mail and emails about the programme and news*

☐ *I give consent to my information being passed to partner organisations who may have products or programmes of potential interest*

The above shows the form that a statement may take. It would have to suit the requirements of the organisation. You don't have to ask irrelevant questions.

Children under 16 (UK may decide 13) cannot give consent, so must get parental consent.

Four technical aspects for the organisation's Committee and Data Protection lead.

Subject Access requests (SAR)

Individuals are entitled to ask for a full record of data held about them. They must be provided with this within 1 month. They can no longer be charged. The information required to be provided is anything that is "Biographical". A document has to have a specific reference to the data subject. Therefore this does not include a name or a passing reference to the person in a report or email.

It is important that when a Subject Access request is made, that the request is verified to come from the data subject. There have been cases of people wanting to find out information held about others. This applies to information about children, when they are the data subject – the SAR must be given to the child and not the parent.

Subject Access requests can be refused or charged for if they are manifestly unfounded or excessive.

Document and file retention times; Organisations are required to keep certain information for either maximum or minimum times. Therefore this links to Data Protection. Any personal data must be kept securely for the whole period of the retention period then it must be disposed of securely.

Here is a selection of the more common document types that relate to voluntary organisations. Organisations may need to consider their document retention in further detail and create a policy.

Committee minutes and decisions, annual accounts	At least 10 years, perhaps permanently
Records of a closed community group or charity	20 years
Bookkeeping records, invoices etc	6 years
Records of services	10 years
Correspondence	If contains personal information then maximum not longer than for lawful purposes in keeping it.
Employers Liability Insurance certificate	40 years
H&S records	3 years
Safeguarding or child attendance records (there will be a difference between simple registers, accident records, safeguarding concerns and investigations)	Depends, organisation must take advice and decide, perhaps for 3 years or until child is 18 or 25 or some say for 100 years
Accident reports	3 years
Contracts	10 years after completion
Employee records, payroll records, pension records	6 years
Sickness records	3 years
Employee work and rest periods	2 years min.
Maternity pay records	3 years
Unsuccessful job applicants	6 months

Reporting Data Breaches to ICO

A data breach is anything that compromises your data including loss, accidental or malicious destruction, unauthorised disclosure of, or access to, personal data. GDPR requires investigation and resolution as well as reporting to the ICO. A breach may require you to inform the person(s) whose data has been compromised. You would be expected to demonstrate that you have the organisational and technical skills to manage this and to maintain data securely in the future. A report of a breach would also have to be made to the Charity Commission.

Security breaches must be reported to ICO within 72 hours unless the loss of data is UNLIKELY to result in risk to data subjects, but there must then be an Internal Breach Register

In practical terms this might mean reporting such as loss of a laptop or pen drive with unencrypted personal data on it, or destruction of a drive with personal data by ransomware, or sending personal data to someone not entitled to receive it. It could be a member of staff sending data home for private purposes – rare, but a conviction was made for this in 2017.

International

Transfer outside the EU is restricted. There must be “adequate protection” of the data. This applies to cloud based solutions etc.

Full information is needed about the systems eg Microsoft, Google or other cloud systems before using them to hold personal data. Responsibility for security is with both the organisation whose members data is stored and with the cloud provider. Data subjects must give their consent to transfer out of the EU. It is sufficient to have a Data Protection Policy that includes Privacy Statement which identifies how data is kept securely and that individuals could withhold permission.

Appendix

About the Lawful bases for Data Processing from the ICO

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ or https://goo.gl/aecXFi

Organisations that keep personal data must first determine why they do that and what the legal basis for keeping the data is. You should record this in your Data Protection Policy and Privacy Statement. You can include several lawful bases, but after starting to collect data you should not change the reason. This is because GDPR requires transparency in the use of personal data.

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

We are grateful to Community First Wessex and Community Action Fareham for producing this fact sheet. (https://www.cfirst.org.uk/ http://www.actionfareham.org.uk/)