Data Protection Update – April 2018

Data Protection refers to the processes that surround the collection, use and storage of data relating to an individual. In 2018 the law changed around Data Protection with the introduction of the General Data Protection Regulation also known as GDPR. This will be enforceable from the 24th May 2018.

Fundamentally the GDPR is similar to existing data protection regulations so organisations that are already following good practice will probably not notice much difference in their practices.

Crucially though there is a requirement for organisations to be transparent in how they process data so that individuals can see what data is collected, for what purpose, how long it is stored and how it is stored. It is therefore a good idea to review your processes and ensure they are clear, concise and accessible.

The GDPR is a piece of legislation from the European Union. After Brexit the UK Government has committed to maintaining the principles of the GDPR and will introduce the Data Protection Bill that will repeal the Data Protection Act and incorporate GDPR.

Data Protection Principles

GDPR sets out data protection principles which outline the main responsibilities for organisations and requires that personal data is:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Suggested steps to take be compliant

1) Data Protection Policy
This should be reviewed in line with the changes and adopted by the Committee/trustee board. It should include:

- Recognition that all data processed should have a "lawful basis" for processing
- A commitment to ensuring that staff/volunteers responsible for processing data have appropriate training
- Recognition of the 8 rights of an individual in relation to their data
- Commitment to keeping up to date records on data processing activities
- Commitment to data protection by default and design
- Commitment to ensuring any organisations that carry our data processing on your behalf are aware of their responsibilities and liabilities in regards data protection.
- Commitment to review the policy annually and ensure it remains current.

It is advisable to refer to "current Data Protection Legislation" within your policy instead of the GDPR to ensure it remains current after Brexit.

2) Data Audit
To help identify your processes around personal data it is recommended that you carry out a data audit. This includes identify what data you hold, how that data is categorised, how it is stored, who can access it, what security you have in place and how long data is retained.

Data you hold could include membership records, donor records, monitoring data for funding applications, records of customers or clients, volunteer contact details and/or photographs

Data Protection legislation only applies to personal data for individuals so business to business data such as funder contacts, utility suppliers, landlord etc may not be subject to the same controls.

A suggested template for this audit and some worked examples is below

Description	Type of data	Why is the data held and what is it used for	Basis for processing data	Who holds the data and who can access it?	What security controls are in place?	How long is data kept for?
Membership records	*Personal data*	*Contact details for members to communicate about organisation activities*	*Legitimate interest*	*Membership secretary is responsible for the data.* *it can also be accessed by the Chair*	*Data held on a password protected database*	*Memberships are renewed annually. Lapsed member data is removed*
Demographic information about members	*Special categories of personal data*	*Age and health information on members to enable feedback to funders*	*Legitimate interest (as defined by Article 9.2 of the GDPR)*	*Membership secretary is responsible for the data.* *it can also be accessed by the Chair*	*Data held on a password protected database*	*Data is anonymised once membership lapses and retained indefinitely.*
Mailing list records	*Personal data*	*Email addresses of supporters and other interested parties*	*Consent*	*Communications secretary maintains the list.*	*Data held on a password protected database*	*As long as consent is in place*

3) Privacy notice
A key element of the GDPR is around transparency of data processing and the recommended way to do this is through a Privacy Notice.

A Privacy notice makes information about how data is used accessible to individuals it is an important step in ensuring fair processing.

The information you have listed in your data audit will form the basis of your privacy notice and you should consider the below questions

Where and how will you collect data?
What information will be collected?
Why is it being collected?
How will it be used?
Who will it be shared with?
How will be stored?
How long will it be stored?
Who can access it?

You should also provide information on “individual rights” and the right to complain to the Information Commissioners Office.

If you have a number of different processes around data protection you may wish to develop separate privacy notices or summaries for each of them to keep things clear for members of the public.

Your privacy notice should be available wherever you collect data. It is also a good idea to make it available on your website for the public to view and should include the contact details of a named person who is responsible for data protection.

Definitions

Personal data - any information relating to a living person who is identified (or can be identified) from that information. E.g. names, addresses, telephone numbers, job titles, date of birth, salary contained in a filing system (e.g. personnel files, online HR records, card indexes)

Special Categories of Personal data – personal data revealing race or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation

In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked.

Data Controller - A controller determines the purposes and means of processing personal data.

Data Processor - A processor is responsible for processing personal data on behalf of a controller.

Data Subject – any living identifiable person about whom personal data is processed

Date Processing – anything done with personal data, this includes; collection, recording and storing, organising and structuring, altering, using, disclosing, erasing and destroying.

Lawful Basis (Article 6) – a valid basis for processing personal data. The GDPR recognises six lawful bases for processing.

Consent – requires a positive opt in, offering choice and control and clear statement of consent
Contract – processing data to fulfil a contractual obligation to a data subject or provide a quote.
Legal Obligation – if you need to process the personal data to comply with common law or statutory obligation.
Vital interests – if you need to process data to protects someone's life
Public Task – in the exercise of official authority

Legitimate interest – the most flexible lawful basis for processing. Likely to be the most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
Legitimate interest could exist where the data subject is a client or in the service of the data controller**.**

Conditions for processing special category data (Article 9) – Additional conditions for lawful processing of special categories or personal data.
Explicit consent
Necessary for carrying out obligations under employment, social security or social protection law
Necessary to protect the vital interests of the data subject
Not for profit membership organisations processing personal data of members or former members

Personal data made public by the data subject
Necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
Necessary for reasons of substantial public interest

Individual Rights - Data subjects have individual rights in relation to their personal data

- a right to be informed as to how personal data is used and stored
- a right of access to any personal data held
- the right for personal data held to be rectified
- the right for personal data to be erased
- the right to restrict the processing of personal data
- the right to data portability
- the right to object
- rights in relation to automated decision making and profiling

More information

The Information Commissioners Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. There is a wide range of information on their website to help organisations to understand and implement GDPR and other data protection legislation.

General
https://ico.org.uk/

Guide for charities
https://ico.org.uk/for-organisations/charity/

Small organisations helpline
0303 123 1113 option **4**