Data Protection for Small and Medium Sized Charities

The Data Protection Act 1998 (DPA) is an Act of Parliament which defines UK law on the processing of data on identifiable living people. It is the main legislation that governing the protection of personal data in the UK. It is a way individuals can control information about themselves and anyone holding personal data for other purposes is legally obliged to comply with it. It requires companies and individuals to protect personal information.

The Act covers any data that can be used to identify a living individual. Anonymised or aggregated data is not regulated by the Act, providing the anonymisation or aggregation is irreversible. Individuals can be identified by various means including their name and address, telephone number or Email address. The Act applies only to data which is held, or intended to be held, on computers, or a 'relevant filing system', including for instance a paper address book or diaries.

The Data Protection Act creates **rights** for those who have their **data stored**, and **responsibilities** for those who store, process or transmit such data. The person who has their data processed rights to:

- View the data an organisation holds on them.
- Request incorrect information be corrected.
- Require that data is not used in any way that may potentially cause damage or distress.
- Require that their data is not used for direct marketing.

Data Protection Principles

Personal data must be processed fairly and lawfully;

- Personal data must be obtained only for one or more specified and lawful purposes, and not further processed in any manner incompatible with that purpose or those purposes.
- Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data must be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Personal data should only be processed fairly and lawfully when;

- Processing is necessary for the performance of, or commencing, a contract;
- Processing is required under a legal obligation (other than one stated in the contract);
- Processing is necessary to protect the vital interests of the data subject;
- Processing is necessary to carry out any public functions;
- Processing is necessary in order to pursue the legitimate interests of the "data controller" or "third parties".

What is personal data?

The definition of personal data is data relating to a living individual who can be identified from that data or from that data and other information in the possession of, or is likely to come into the

possession of, the data controller. Sensitive personal data concern the subject's race, ethnicity, politics, religion, trade union status, health, sex life or criminal record.

Consent

An individual needs to consent to the collection of their personal information and its use in the purpose(s) in question. Consent is "…any freely given specific and informed indication of an individuals' wishes by which the data subject signifies his agreement to personal data relating to them being processed", meaning the individual may signify agreement other than in writing. However, non-communication should not be interpreted as consent.

The consent should be appropriate to the age, capacity and circumstances of an individual for example if an organisation "continues to hold or use personal data after the relationship with the individual ends, then the consent should cover this." Even when consent is given, it shouldn't be assumed to last forever. Although in most cases consent lasts for as long as the personal data needs to be processed, individuals may be able to withdraw their consent, depending on the nature of the consent and the circumstances in which the personal information is being collected and used.

The Data Protection Act also specifies that sensitive personal data must be processed according to a stricter set of conditions, in particular any consent must be explicit.

Top Tips

1. **Tell people what you are doing with their data**
   People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice) so it is important you are open and honest with people about how their data will be used.

2. **Make sure your staff are adequately trained**
   New employees must receive data protection training to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff.

3. **Use strong passwords**
   There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep your information secure from would-be thieves.

4. **Encrypt all portable devices**
   Make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.

5. **Only keep people's information for as long as necessary**
   Make sure your organisation has established retention periods in place and set up a process for deleting personal information once it is no longer required.

For further support and advice visit https://www.gov.uk/data-protection/the-data-protection-act or get in touch with funding@savs-southend.co.uk.