Managing your charity's data… and reputation

The fundraising scandal has shone a light on data protection issues and charities' compliance with data protection law is increasingly being called into question. In addition to the potential legal consequences, charities need to be aware of the reputational impact non-compliance can have.

In recent months, the Information Commissioner's Office (ICO) has been a hive of activity, updating its encryption guidance and direct marketing guidance. It also updated its privacy notices code, its checklist for selling and buying data, and its standard wording for organisations to use when collecting personal data for marketing purposes.

It is essential that charities keep up to date with ICO guidance and have robust policies and procedures in place to manage their data and ensure public confidence.

The legal requirements

Organisations are subject to the Data Protection Act 1998 (Act) and The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). Both the Act and PECR set out principles which organisations must follow, but the law does not prescribe specific actions organisations must take in order to ensure compliance.

The ICO, as the regulator and enforcer of data protection law, issues guidance on how organisations must behave in order to comply with the law. Some guidance is defined as 'Code of Practice' which means it has specific statutory recognition and can be considered by the courts. It can sometimes be difficult to draw a line between what is a strict legal requirement and what is only guidance.

It is possible to challenge the ICO's guidance but we would generally recommend that organisations keep up to date with and follow the guidance.

Recently updated guidance and taking steps to comply with the law

With this in mind, we have summarised two areas of guidance recently updated by the ICO.

Encryption of devices - The seventh data protection principle states: "*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.*"

The ICO's encryption guidance (amongst other guidance) sets out the steps organisations should take in order to adhere with this requirement. Without any encryption, an organisation would be vulnerable to third parties accessing their data. Encryption is widely available and committing resource to ensure data is encrypted will help organisations be compliant with the seventh data principle. Often data protection breaches and subsequent ICO enforcement derives from lost unencrypted memory sticks, work phones or laptops. These types of breaches should be easily avoidable.

Obtaining Consent - The first data protection principle states that "*personal data shall be processed fairly and lawfully*". This principle can be complied with by meeting one or more of

several specified conditions. One of those conditions that an organisation may have to rely on is 'consent' – working out exactly what 'consent' means is complex. The definition of consent is "*any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed*". Over the years, the ICO has taken a stricter view on what it deems to be valid consent. Organisations should treat 'implied' consent with caution. For example, a person signing up to a campaign should not automatically be taken as having given consent to be contacted about other campaigns or other activities of the organisation.

Organisations now need to be far more specific in terms of the consent they get from an individual, before using the individual's data. Detailed information should be provided where any data may be shared with third parties and in each case the data subject should be given the ability to opt-out of such processing. Broad statements such as *"we share your information with authorised/selected third parties"* are unlikely to be deemed acceptable by the ICO.

New law: The EU General Data Protection Regulation

Current data protection laws derive from an EU Directive which came into effect in 1998. The EU has just agreed the final version of the Data Protection Regulation & Directive (the Regulation) which will come into force from 25 May 2018. It introduces some significant changes and it is important that organisations understand the new rules and change their data protection policies and practices so they are compliant.

Key changes are:

Governance - Organisations will have increased responsibility and accountability on how they control and process personal data.

Consent - The Regulation requires a more active form of consent to fulfil the requirement of lawful processing of personal data; wherever consent is required for data to be processed, consent must be explicit, rather than implied.

Enforcement - Non-compliance will likely lead to higher sanctions. The current maximum fine is £500,000. The maximum fine will be increased up to 4% of the annual worldwide turnover of an organisation or €20 million euros (whichever is the greater). A data subject also has the right to bring court action against an organisation if it infringes the Regulation.

Compulsory data protection officer - Organisations will need to appoint a Data Protection Officer (DPO) when they are, for example, processing sensitive data. The DPO must report to the highest management level in an organisation.

Privacy impact assessment (PIA) - Where operations present higher privacy risks to data subjects, a PIA will be a compulsory precondition before an organisation can carry out the relevant operation.

Privacy by design and privacy by default - When developing a new product or service, organisations need to take privacy risk into account. Procedures should be adopted to ensure that, by default, minimal personal data is collected, used and retained.

The right to be forgotten - The Regulation provides data subjects with the 'right to be forgotten', allowing data subjects the right to have data files relating to them deleted if there are no 'legitimate grounds' for retaining them.

Transparency of privacy notices - Organisations will have increased transparency obligations towards data subjects; privacy notices (for example the statement provided in forms which collect data) will need to include much more detailed information than at present.

Data processors - A welcome change is that data processors (in addition to data controllers) will have obligations to fulfil under the Regulation and will be liable to sanctions if they fail to meet them.

With these big changes on the horizon it will be very important for organisations to review their data protection policies and procedures. Data protection is an increasingly prominent issue in the sector (and in the press), and proper data management is a key way in which charities can protect or even enhance their public image.

We regularly assist organisations with data protection audits in order to identify any potential risks. Once a thorough audit has been undertaken, the charity can implement operational changes to confidently guard against these risks and ensure compliance with both current and future regulation.

Andrew Studd
Partner
+44 (0)20 8394 6414
Andrew.Studd@russell-cooke.co.uk

Victoria Ehmann
Associate
+44 (0)20 8394 6464
Victoria.Ehmann@russell-cooke.co.uk