yeomans

Data cleansing and consent

Get it Right! (February 2017)

Following news towards the end of 2016 of monetary penalty notices being issued by the Information Commissioner's Office (ICO) to the RSPCA and British Heart Foundation (BHF) due to contraventions of data privacy principles, there is much concern regarding how organisations are allowed to gather, store and use the personal information of their supporters.

3 Major Data Protection Act Breaches:

We understand that the RSPCA was fined £25,000 and BHF £18,000 (both of which had these fines reduced due to swift settlement) and that these fines were brought about as a result of specific data protection breaches including:

- Carrying out "Wealth Screening" and failing to handle donors' personal data consistently with legislation
- Tracing and targeting new or lapsed donors by piecing together personal information obtained from other sources to obtain data that had not been provided by the donor
- Trading personal details through a scheme in which charities could share or swap personal data to get details of prospective donors. Whilst donors were given the opportunity to opt out of allowing their data to be shared with "similar organisations" it was felt that the description used did not provide enough information to enable people to make a decision to opt out

In each of the above situations, donors were not informed of the practices so were unable to consent or object.

These high profile cases have understandably thrown the industry into turmoil as there is much concern about what is and is not considered to be lawful processing of data.

We wish to support our clients and ultimately do all we can to ensure that no one falls foul of the Data Protection Act, therefore we have been working through the guidance and regulations carefully for you.

Major duties of charities under the Data Protection Act 1998 (DPA):

These cases have obviously brought 3 specific areas of Data Protection legislation into the spotlight, whilst reminding charities of their major obligations under the DPA. These can be read in full in the ICO Guide to Data Protection and are stated below:

1) Where organisations hold data about their supporters, they are "data controllers" - As a data controller it is an organisation's duty to comply with data protection principles in relation to all the personal data they hold or control

2) The DPA must be applied so as to ensure the protection of an individual's fundamental rights to the protection of their personal data

3) Charities have a duty to uphold the 8 data protection principles which, (according to the ICO) are as follows:

   A. **Personal data shall be processed fairly and lawfully** and, in particular, shall not be processed unless:

      i. At least one of the conditions in Schedule 2 is met. These conditions are:

         1. That the data subject has given their consent to the processing
         2. The processing is necessary for the performance of a contract or because the data subject has asked for something to be done so they can enter into a contract
         3. The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract)
         4. The processing is necessary to protect the vital interests of the data subject, (this only applies in cases of life or death)
         5. Data processing is necessary for the administration of justice, or for exercising statutory, governmental, or other public functions
         6. Data processing is necessary for the purposes of legitimate interests pursued by the data controller

      ii. In the case of sensitive personal data, at least one of the conditions in Schedule 3 must also be met. These conditions are:

         1. The data subject has given their explicit consent to the processing of their personal data
         2. The processing is necessary so that you can comply with employment law
         3. Processing is necessary in order to protect the vital interests of the data subject or another person
         4. The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject

6. Processing is necessary for the purpose of any legal proceeding

7. Processing is necessary for administering justice

8. Processing is necessary for medical purposes and is undertaken by a health professional

9. The personal data is processed for monitoring of equality of opportunity and carried out with appropriate safeguards in place

B. **Personal data shall be obtained only for one or more specified and lawful purposes**, and shall not be further processed in any manner incompatible with that purpose or those purposes

C. **Personal data shall be adequate, relevant and not excessive** in relation to the purpose or purposes for which they are processed

D. **Personal data shall be accurate** and, where necessary, kept up to date

E. **Personal data processed for any purpose or purposes shall not be kept for longer than is necessary** for that purpose or those purposes

F. **Personal data shall be processed in accordance with the rights of data subjects** under this Act. The rights of individuals that this section of the act refers to are:

   i. a right of access to a copy of the information comprised in their personal data

   ii. a right to object to processing that is likely to cause (or is causing) damage or distress

   iii. a right to prevent processing for direct marketing

   iv. a right to object to decisions being taken by automated means

   v. a right (in certain circumstances) to have inaccurate personal data rectified, blocked, erased or destroyed

   vi. a right to claim compensation for damages caused by a breach of the Act

G. **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.

H. **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.

As a result of these high profile cases surrounding donor consent, many organisations are questioning their handling and storage of supporter data to ensure that they comply with the principles and framework above.

Having reviewed the penalty notices issued by the ICO in these cases and the consent statement guidelines issued by the NCVO (which can be accessed here) our current recommendations for ensuring you comply with the current guidance and regulations are as follows.

8 Tips to ensuring you're DPA compliant

1. When asking your supporters (in writing) for their consent to receive correspondence from you, make sure you are clear in what you are asking

2. Give your supporters clear opportunity to give their informed consent for their data to be used in specified ways

3. Give new supporters the opportunity to opt-in to receive communications from you (do not assume they've given consent because they've not opted-out of communications) – If you're concerned that people may not choose to tick an opt-in box, try making a feature of it by showing its value to the donor (ie: by ticking this box we can keep you up to date with important news about how your support is changing lives). Please note: Whilst supporters can (currently) be contacted by post without specifically opting-in, it is essential that in the case of electronic marketing communications, supporters MUST have opted-in to receive them

4. For your existing supporters, if you don't have their explicit consent to receive specific marketing messages you need to be able to demonstrate that they have given valid/implied consent to receive your communications

5. For previous supporters who have been mailed (repeatedly) but not responded directly you should not assume you have their implied consent to continue sending them marketing communications - These individuals should be treated as potential new supporters and given the opportunity to opt-in to future communications

6. Donors should not have their data screened against wealth, income and household tenure etc. for the purpose of gaining funds unless they have specifically given informed consent for you to do so

7. Without informed and explicit consent it would be unlawful to process data to enhance it

8. Whilst there is no fixed time limit after which consent automatically expires, it is recognised that consent will not remain valid forever. The National Council for Voluntary Organisations (NCVO) has recommended that large fundraising organisations should refresh the consents they use to contact donors by phone every 24 months, whilst the ICO recommends that as a general rule of thumb, if an organisation is making contact by phone, text or email for the first time, it does not rely on any indirect consent given more than six months ago

The guidance on data storage and processing can seem like a minefield and is frequently changing. For up to date information and to discuss the practical implications for your specific organisation please contact us, or register to attend our next workshop.

References:

The ICO guide to data protection can be viewed at https://ico.org.uk/for-organisations/guide-to-data-protection/

DMA – Data protection toolkit can be viewed online at https://dma.org.uk/product/data-protection-toolkit

NCVO guidelines for donor consent can be found at https://www.ncvo.org.uk/images/images/about_us/media-centre/NCVO_-_Charities_relationships_with_donors.pdf

t 01892 839280
e sales@weareyeomans.co.uk
weareyeomans.co.uk
Head Office and Reception: Suite 1 **Production:** Unit 12
Branbridges Industrial Estate, East Peckham, Kent TN12 5HF

Yeomans Press Ltd Registered Office: 3 Boyne Park, Tunbridge Wells, Kent TN4 8EN Registered No: 5306145 VAT No: 821 7544 35