DATA PROTECTION

A GUIDE FOR CHARITIES AND NON-GOVERNMENTAL ORGANISATIONS

JUNE 2018

REUTERS/PAWEL KOPCZYNSKI

THOMSON REUTERS FOUNDATION

CMS Law.Tax

dentsu AEGIS network

ACKNOWLEDGEMENTS

The Thomson Reuters Foundation is extremely grateful to the following authors of this Guide for their time and expertise, which made this Guide possible:

CMS Law.Tax

Duncan Turner
Joy Black
Claire Brown

dentsu AEGIS network

Mahisha Rupan
Hannah Wilkinson

THOMSON REUTERS®

Erika Hayes

DISCLAIMER

This guide has been produced by the Thomson Reuters Foundation, Dentsu Aegis Network and CMS Cameron McKenna Nabarro Olswang LLP. It has been written for charities and non-governmental organisations (NGOs) for general information purposes only and nothing contained in this guide is intended to provide legal or other professional advice.

The Thomson Reuters Foundation, Dentsu Aegis Network and CMS Cameron McKenna Nabarro Olswang LLP do not accept any responsibility or liability for any loss which may arise from reliance on information contained in this guide.

ABOUT US

THOMSON REUTERS FOUNDATION

The Thomson Reuters Foundation acts to promote socio-economic progress and the rule of law worldwide. The Foundation runs initiatives that inform, connect and ultimately empower people around the world: access to free legal assistance, media development and training, editorial coverage of the world's under-reported stories and the Trust conference.

TrustLaw is the Thomson Reuters Foundation's global pro bono legal programme. We connect high-impact NGOs and social enterprises working to create social and environmental change with the best law firms and corporate legal teams to provide them with free legal assistance. With a presence in over 175 countries, we support more than 3,600 organisations with free legal assistance. Our free legal service enables NGOs and social enterprises to streamline operations, expand into new countries and scale their impact. This helps them focus on their mission without spending valuable resources on their legal needs. TrustLaw also produces a wide range of tools to help NGOs and social enterprises address their legal needs and support their advocacy efforts. NGOs and social enterprises are under constant pressure to keep pace with complex legal developments. The General Data Protection Regulation which was introduced in May 2018 brings into force a host of legal requirements that will affect organisations that process data in the European Union. TrustLaw is committed to supporting affected NGOs and social enterprises by providing this Guide, as well as a suite of other guides, resources, interactive tools and training. These are designed to make it as easy as possible for NGOs and social enterprises to prepare for new laws and achieve their goals.

To learn more, take a look at our website at www.trust.org.

CONTENTS

INTRODUCTION

People expect organisations to treat their data well. So, knowing how to treat data about the people who work with and support you is important. This guide provides charities and NGOs with an introduction to the data protection rules that govern the way they collect and use personal data. More specifically, it aims to help charities and NGOs in meeting their obligations under data protection legislation in the UK.

1. WHAT IS DATA PROTECTION?

Data protection is a term used to describe the lawful handling of data about living people. For charities and NGOs, those people will include staff, volunteers, donors, suppliers and users of their services (the data subjects).

What laws apply in relation to the collection and use of personal data by charities and NGO?

In the UK, the main pieces of legislation governing data protection are:

- the General Data Protection Regulation, regulation (EU) 2016/679 (the **GDPR**); and
- the Data Protection Act 2018 (the **DPA 2018**) (together, for the purposes of this guide, they are referred to as **Data Protection Laws**).

The GDPR is an EU regulation which applies directly to all EU member states. In addition to the GDPR, member states may enact national legislation to supplement the GDPR. Indeed, the UK has enacted supplemental legislation known as the DPA 2018. There may be national legislation relating to data protection in other EU countries, which apply to your organisation; however, this guide focuses on data protection requirements in the UK.

Data Protection Laws give people more control about how their data is used. In particular, the Data Protection Laws require organisations to be accountable and transparent about how they use data.

In addition, there are also the Privacy and Electronic Communications (EC Directive) Regulations 2003 (**the Privacy Regulations**). The Privacy Regulations sit alongside the Data Protection Laws and give individuals specific privacy rights in relation to electronic communications. The Privacy Regulations contain specific rules on: marketing calls, emails, texts and faxes; cookies (and similar technologies); keeping communications services secure; and customer privacy as regards traffic and location data.

What type of data is covered by Data Protection Laws?

Data Protection Laws are concerned with **personal data**. This is data about a living person (i.e. data subjects). It covers:

- data that clearly relates to a person – such as their name and email address;
- data that by itself won't identify a person, but which could identify a person when combined with other information that an NGO or charity holds within its files and systems. For example, an NGO or charity may hold records that do not identify a person by name. Instead those records bear unique reference numbers that, when matched to another data set on file, identify the people concerned.

Further guidance on determining what constitutes personal data can be found on the Information Commissioner's Office's (the ICO) website, available at https://ico.org.uk/media/for-organisations/documents/1549/determining_what_is_personal_data_quick_reference_guide.pdf.

What activities are regulated by Data Protection Laws?

Data Protection Laws regulate the "processing" of personal data. Processing should be interpreted broadly, covering everything that a charity or NGO does with data – from collecting the data, storing the data, using the data and then, finally, destroying the data.

Who do Data Protection Laws apply to?

Data Protection Laws apply to NGOs and charities that are established in the UK. However, NGOs and charities that are based outside of the UK are also caught by the law: to the extent they process personal data relating to EU data subjects, they will be subject to the GDPR.

What are the principles at the heart of data protection?

There are six principles that NGOs and charities must follow when processing personal data. These principles are set out in the DPA 2018, and summarised below:

1. Processing must be done fairly, lawfully and in a transparent manner. This means two things:
    - » being transparent with the people who have shared their personal data with you. NGOs and charities should be upfront as to how personal data will be processed, for what purpose and whether it will be shared with anyone else. Privacy notices provide a good way to communicate this type of information – the ICO has produced a helpful guide on privacy notices on the ICO's website, available at https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/; and

- having a lawful basis on which to process the personal data of data subjects. There is a number of lawful bases that could be relied upon. For example, the NGO or charity has a legitimate interest in processing the personal data, or the NGO or charity has obtained the consent of the data subject.

The processing of **special categories of personal data** (such as data about a person's racial or ethnic origins, political opinions or sexual life) is subject to further conditions.

The ICO has produced guidance on the conditions for processing personal data , available at https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/.

2. Personal data must be acquired for a clear and specified purpose. For example, it cannot be collected for one purpose only to be used for another purpose. NGOs and charities must use personal data in the way they told data subjects it would be used.

3. Personal data collected shall be adequate, relevant and not excessive. NGOs and charities are collecting personal data for a specific purpose(s) – they should collect the minimum amount of data necessary to achieve that purpose(s).

4. Personal data must be accurate and kept up to date.

5. Personal data should not be kept longer than is necessary. NGOs and charities should be deleting personal data when it is no longer required.

6. Personal data must be kept secure. NGOs and charities should ensure that they have robust physical and technical security measures to protect the personal data.

2. WHY IS DATA PROTECTION IMPORTANT?

Charities and NGOs can reap the benefits and mitigate risks by complying with Data Protection Laws.

What are the benefits of ensuring data protection compliance?

- Personal data is a key asset for charities and NGOs. Handling it properly will help your organisation to achieve its objectives.
- Data protection compliance means good data management which can, in turn, save your organisation time, effort and money.
- If you can demonstrate the protection of data subjects' personal data, you will develop and maintain trust and confidence in your organisation.

What are the risks of getting it wrong?

- There may be serious financial and reputational costs for failing to comply with Data Protection Laws. A data breach can be expensive to put right and will reduce public confidence in your organisation. Additionally, a breach of the GDPR puts your organisation at risk of receiving significant monetary penalties. Regulators can impose fines for serious breaches of up to €20million or 4% of an organisation's global turnover.

3. WHAT DO DATA PROTECTION LAWS REQUIRE?

The Data Protection Laws came into effect this year. They introduce obligations that your charity or NGO may not have been subject to under old data protection laws. These new obligations are detailed below.

- **Accountability is key.** NGOs and charities cannot merely say they comply with the Data Protection Laws – they must be able to demonstrate compliance through data protection policies, training and record keeping. The ICO provides further information on the GDPR accountability principle on their website, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/.
- **Fines.** Up to the higher of 4% of global turnover or €20million for serious breaches.
- **Clearer expression of "consent" will be required.** Under the GDPR, consent means any **freely given**, specific, informed **and unambiguous** indication of a person's wishes by which he or she, **by a statement or by a clear affirmative action**, signifies agreement to the processing of their data.

  Individuals must not feel forced to consent to their data being used by you. Individuals must also be able to withdraw their consent to your use of their data at any time.

  The way in which data is collected should leave no room for doubt that an individual has consented to how their data will be processed. Separate consents should be obtained for distinct processing activities.

  There must be a positive indication that an individual has consented. Silence will not constitute consent. Nor will pre-ticked opt-in boxes.

- **Privacy-by-design:** The GDPR provides that a data protection impact assessment should be conducted in certain circumstances. This is to ensure privacy is factored into new initiatives from the start – privacy should never be an afterthought. See the ICO's guidance at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ for help in determining whether you should conduct a data protection impact assessment.
- **Data Protection Officers (DPO).** There are certain circumstances when it is mandatory to appoint a DPO. For example, where special categories of personal data are processed by an organisation on a large scale, including data relating to health or criminal convictions.
- **A wider definition of personal data.** An organisation now has data protection obligations in relation to a wider set of data. For example, the GDPR's definition of personal data makes it clear that information such as an online identifier (for example, an IP address) can be personal data. The GDPR allows for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

4. WHAT PRACTICAL STEPS SHOULD CHARITIES AND NGOS TAKE TO COMPLY WITH THE DATA PROTECTION LAWS?

1. **Training.** Make sure that people in your charity or NGO are aware of Data Protection Laws. Where you have created new internal policies to help drive data protection compliance within your organisation, make sure they are implemented. Training is important here. You should also keep a record of any data protection-related training delivered to your staff – this will help to evidence your compliance.

2. **Keep a record of personal data that you store and use.** Charities and NGOs should know who their data subjects are, as well as how and why their data is collected and used by your organisation. You should also document where the data came from and who it's shared with.

3. **Ensure you have the required contractual arrangements in place.** The Data Protection Laws require that charities and NGOs put in place effective contract documentation for the processing or sharing of personal data with other organisations (e.g. where you transfer data to a supplier so that they can provide you with a service).

   Where you share data with other organisations, you will need to ensure that there is a written agreement in place with those organisations. Or, if there is an existing agreement, be sure to incorporate the necessary processing provisions. The ICO explains what you must include in such agreements in order to comply with the Data Protection Laws: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/.

   Additionally, personal data relating to EU data subjects may only be transferred outside of the EU when done in compliance with the specific conditions set out in the Data Protection Laws. The ICO discusses international transfers of data, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/.

4. **Be transparent about your data processing activities.** Charities and NGOs should be upfront with data subjects about how personal data will be processed, for what purpose and whether it will be shared with anyone else. Privacy notices are the best way of communicating this type of information. Review your current privacy notices against the requirements of the Data Protection Laws, update them if necessary and then make sure they are shown to data subjects in a timely manner. The ICO has produced a helpful guide on privacy notices, on their website, available https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/.

5. **Put in place processes to comply with data subject access requests.** Data subjects have a right to request access to their personal data. In preparation for receiving these types of requests, please bear in mind the following:

    - *Fees.* Some European laws previously permitted data controllers to charge a fee for dealing with a data subject access request. Now, however, fees may not be charged unless the access request has no clear basis in fact, is excessive, or where the data subject has asked for additional copies of the requested information.
    - *Time to respond.* NGOs and charities must respond to a data subject access request "without undue delay" and at the latest within one month of receipt of the request. While it may be possible to request an extension in certain circumstances, the time to respond could represent a change for some organisations.

    You should make sure that relevant policies and procedures are updated to reflect these new data subject access requests requirements.

6. **Prepare for new and enhanced data subject rights.** The Data Protection Laws create new rights for data subjects and strengthen certain rights that existed under previous data protection law. We've already touched upon data subject access requests. There are, however, other rights that your organisation should prepare for. For example, data subjects may have the right to request that an NGO or charity delete their personal data. The ICO explains these rights and provides checklists: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

7. **Make sure you have a legal basis for processing personal data.** Having documented the type of personal data that your organisation uses (see point 2, above), you should identify a legal basis for that use. Use this guide from the ICO to determine the most appropriate legal basis: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

8. **Think about consent.** If your legal basis for processing personal data is 'consent', you should review your consent mechanism – it needs to meet the criteria described in Section 3. For guidance on consent, see this ICO guide: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

9. **Prepare for data breaches.** Organisations have an obligation to inform regulators (and in some circumstances, data subjects) about data breaches. Make sure you have in place the means to detect breaches, investigate breaches and to report those breaches within 72 hours. Use the checklist at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ to prepare.

As well as detecting breaches, it is just as important to prevent breaches. Charities and NGOs should implement security measures to ensure a level of security appropriate to the risk. The more sensitive the data you store, the more robust the security measures implemented. For more information on security, see this ICO guide: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

10. **Know when to carry out a data protection impact assessment.** Data protection needs to be considered at the outset of a project – data protection impact assessments help you to identify and minimise the data protection risks. Make sure your organisation knows when to carry out this type of assessment – see the ICO's guidance here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

11. **Consider if it's necessary to appoint a DPO.** Again, the ICO's guidance will help you to determine if a DPO should be appointed: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

12. **Treat children as vulnerable persons.** If you are collecting data directly from children (in the UK, a child is defined as under the age of 13 – but this definition changes by country), make sure it is done fairly. Consider if systems should be implemented to verify data subjects' ages or to obtain parental or guardian consent to the processing of children's data (see section 7 for more detail).

13. **Determine if the ICO is your supervisory authority.** If your organisation is based in the UK only, the ICO is your supervisory authority. If your organisation operates internationally, your organisation may fall under the jurisdiction of another data protection supervisory authority.

5. KEY QUESTIONS TO ASSIST WITH COMPLIANCE

When thinking about compliance with Data Protection Laws, your organisation should work with staff to determine answers to the below list of questions.

1. **What personal data does the charity or NGO hold?**
    a. Whose personal data do you collect (e.g. employees, volunteers, service users, donors etc.)?
    b. What types of personal data do you collect (e.g. name, address, date of birth, payment details etc.)? (See Section 4.2 above).
    c. Do you collect any special categories of personal data (e.g. racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health and data concerning a person's sex life or sexual orientation)?
    d. Do you collect or use personal data of children or vulnerable adults? (See Section 4.12 above).
    e. How do you collect personal data (e.g. directly from the data subject, from a third party (e.g. social worker, school etc.) or from a relative or guardian of the data subject)?
    f. Do you use/operate CCTV?
    g. Can you minimise the personal data you collect (e.g. is all personal data you collect required)?

2. **How does the charity or NGO process personal data?**
    a. What is the purpose for collecting/using the personal data?
    b. Do you have a legal basis for collecting/using this personal data? (See Section 4.7 above).
    c. Do you process personal data on behalf of another organisation?
    d. How do you ensure that personal data is kept up to date and accurate (e.g. by contacting data subjects periodically to make sure their details are correct or providing online access to an account that they can update)?

3. **Does the charity or NGO have the necessary information notices and consents?**
    a. Do you have a privacy notice? (See Section 4.4 above).
    b. Has the data subject been told for what purposes you will be using their personal data?
    c. Do you have an internal privacy policy for staff (e.g. employees, contractors and volunteers)?
    d. Do you have signs/notices informing data subjects that you will be collecting CCTV data (if applicable)?
    e. Do you rely on consent to process personal data? If so, does your process for collecting consent comply with the requirements under GDPR? (See Section 4.8 above).

f. If you rely on consent, how do you record consent?

g. If you rely on consent, are data subjects told that they can withdraw their consent at any time and do you have a process for dealing with withdrawals of consent?

h. Do you use personal data for marketing communications? Do you have the appropriate consents for marketing?

4. What technical and organisational measures does the charity or NGO have in place to protect personal data?

a. What security measures do you have in place to protect personal data? (See Section 4.9 above).

b. How frequently do you review and test the security measures you have in place? How is this documented?

c. Do you have internal policies informing staff about how to keep personal data secure?

d. Do you provide training for staff to inform them of good practices to keep personal data secure? (See Section 4.1 above).

e. What special protections do you have in place to protect special categories of personal data?

f. Do you have a documented action plan or policy for dealing with a data security breach?

5. Does the charity or NGO share personal data?

a. Do you disclose personal data to any other organisation (e.g. service providers) for processing on our behalf or for any other use?

b. If so, are there written agreements in place for the processing/transfer of data? (See Section 4.3 above).

c. Do you transfer personal data outside the EEA? For example, to servers hosted outside of the EEA? If so, how do you ensure compliance with the rules on overseas transfers of data? (see Section 4.3 above)

d. Whose responsibility is it to respond to requests from data subjects? (See Section 4.5 above).

e. Do you provide training to staff on data subject rights?

6. How does the charity or NGO deal with compliance and accountability?

a. Do you have a process and/or policy for data retention to ensure that personal data is not processed for longer than is necessary?

b. What do you do with data after it is no longer needed? Do you securely delete it or anonymise it?

6. STARTING A NEW CAMPAIGN

Data Protection Laws include rules that apply to the marketing activities of charities and NGOs. These are detailed below:

Finding new potential donors

When starting a new campaign, you should consider how potential donors are identified and contacted.

1. **Publicly available email addresses or telephone numbers are protected under Data Protection Laws.** All data about individuals, whether publicly available or not, is protected under Data Protection Laws. Therefore, use of personal data from public resources, like LinkedIn, must comply with the Data Protection Laws.

2. **Third party lists.** Take care when buying lists of prospective donors from third parties for emails or marketing calls. These third parties must demonstrate that they have lawfully obtained the data and the data can be used for this purpose.

Telephone marketing (live calls, not automated)

There are additional rules for when you are contacting potential donors by telephone.

1. Charities and NGOs should **NOT** make unsolicited marketing calls to:

    a. an individual or an organisation who has said that they do not want your calls (see Suppression lists below); or

    b. any number registered with the Telephone Preference Service (TPS) or Corporate Telephone Preference Service (CTPS) – even if they are an existing customer (see TPS below).

2. **Suppression lists.** You must not call anyone who has previously objected to receiving marketing calls or emails. Charities and NGOs should maintain an accurate and up-to-date suppression list to record individuals who have objected to being contacted for marketing purposes.

3. **TPS.** TPS is a central register of individuals who have opted out of receiving marketing calls. The TPS list contains details of individuals, partnerships and sole traders who have opted out of receiving marketing calls. Contacting individuals or companies listed on TPS is a breach of the Privacy Regulations.

4. **Be open about where you are calling from.** You must always say who is calling, the company name, allow your telephone number to be displayed to the person receiving the call and provide a contact address or freephone number if asked.

5. **Consent.** If you are contacting a named individual (e.g. Joe Bloggs), then you must comply with Data Protection Laws. In particular, the individual should be aware that you have their number and plan to use it for marketing purposes and should have consented to such contact prior to receiving the call. At the start of the call, please communicate the following to the individual receiving the call:

    a. Your name and organisation.

    b. The purpose for the call, what you plan to do with their data, who you will share it with and how long you are going to keep it for (plus other information required by Data Protection Laws)

    c. Ask the individual if they agree to being contacted by phone for this purpose or if there is another way that they would prefer to be contacted.

6. **Please adhere to the individuals' instructions.** If they ask not to be contacted, please ensure that they are added to the suppression list and not contacted in future. If they ask to be contacted by email, please do that instead.

Email marketing

1. **Consent.** As a general rule of thumb, you cannot send marketing emails without the prior opt-in consent of the individual. Under the Privacy Regulations, there are notable exceptions to the opt-in consent, so please check whether these might apply.

2. **Opt-outs.** Individuals have the right to ask you to stop sending them marketing. If this occurs, make sure that the individual's details are added to the suppression list.

3. **Compliance with Data Protection Laws.** In addition to the above, charities and NGOs must ensure compliance with the Data Protection Laws. Where a charity or NGO is the controller of personal data, such as email and telephone numbers of data subjects, it will have obligations under the Data Protection Laws in relation to that data.

Additional guidance about consent

As previously mentioned, the standard for consent under Data Protection Laws has changed – this also impacts the standard for consent under Privacy Regulations. Therefore, marketing consents must be freely-given, specific, informed unambiguous and should involve a clear affirmative action. You need to review existing marketing consents and your consent mechanisms to check they meet the Data Protection Laws standard. If they do, there is no need to obtain fresh consent.

Additional guidance on Profiling

Data Protection Laws contains specific rules around profiling individuals if the profiling involves automated processing of personal data (i.e. use of personal data without human intervention) and this profiling produces legal effects or significantly affects the individual. Therefore, if you are considering activities that would involve profiling individuals to ascertain their financial status or propensity to donate, further guidance may be needed.

More information

For more information on direct marketing (including specific guidance for charities), please see the ICO guide on this topic, available at https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf.

7. CHILDREN'S DATA

Data Protection Laws introduce new obligations for organisations processing children's data. The rationale for this is that "*children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data*".

The ICO emphasises that as children need particular protection when processing and collecting personal data, organisations should ensure that this is borne in mind at the outset when designing systems and processes relevant to children. Consulting with children when designing systems and processes should be undertaken as a matter of good practice. The ICO further recommends data protection impact assessments are conducted in order to identify and mitigate any data protection risks to children as well as ensuring that any children and their parents are made aware of how the personal data is being used and the risks involved.

When using data about children, charities and NGOs still require a legal basis for using that data. Additional consideration must be given to the following:

- Does the child have the capacity to consent (if consent is the lawful basis for processing being relied upon)? Where a child is not competent to understand what they are consenting to then parental consent will be required in order for the consent to be considered "informed" and valid.
- Does the child have the competence to agree to a contract if "performance of a contract" is being relied on as the lawful basis for processing?
- Where "legitimate interests" is the lawful basis for processing, then processors must ensure that they balance their legitimate interests in processing against the interests and fundamental rights and freedoms of the child. It is the responsibility of the controller to protect the child from any risks associated with processing and to identify any appropriate safeguards. In practice, this means that any processing system should be designed with the need for increased protection for children in mind and in particular the likely need for even greater protection for younger children.

There are additional rules for the use of children's data by an information society service (which is normally an online service). Where information society services are provided to a child, the consent must be provided by the person holding parental responsibility for that child. In the UK, children are those aged 13 years or under, but this varies across the EU.

8. SANCTIONS / REGULATOR ACTION AGAINST CHARITIES

Some charities have come under the spotlight for their failure to comply with Data Protection Laws. In this Section, we highlight the types of practice that have resulted in the ICO taking action against charities.

Fundraising

The ICO lists three things that charities have been doing without the knowledge or consent of donors:

1. Ranking people based on their wealth.
2. Acquiring personal data about people that they did not provide.
3. Sharing data with other charities.

For further information on this, take a look at the guidance here: https://ico.org.uk/for-the-public/charity-fundraising-practices.

Direct marketing

Some charities wrongly believe that the Privacy Regulations do not apply to their promotional activities. Charities have found themselves falling foul of the law when:

1. They have not made it clear to donors/supporters that their details will be used for marketing purposes.
2. Making marketing emails, texts, faxes, or automated calls without the prior consent of the people being targeted.
3. Neglecting to screen their database of phone numbers against the TPS and subsequently targeting people who have opted out of marketing calls.

9. USEFUL RESOURCES

The purpose of this guide is to provide general information on data protection in the UK for charities and NGOs. For additional resources relating to data protection and further information on complying with Data Protection Laws, please see the list below.

Information Commissioner's Office website, which has:

- Charity sector guidance, such as Fundraising and regulatory compliance paper. ICO guidance on various topics, such as direct marketing and CCTV.
- General guide to data protection.
- A self-assessment toolkit for small and medium enterprises.
- Advisory visits to your organisation for a day with a short follow up report.
- An advice service by phone on 0303 123 1113 or 01625 545 745 or email casework@ico.org.uk

The Fundraising Regulator Code of Practice.

THOMSON REUTERS
FOUNDATION

www.trust.org