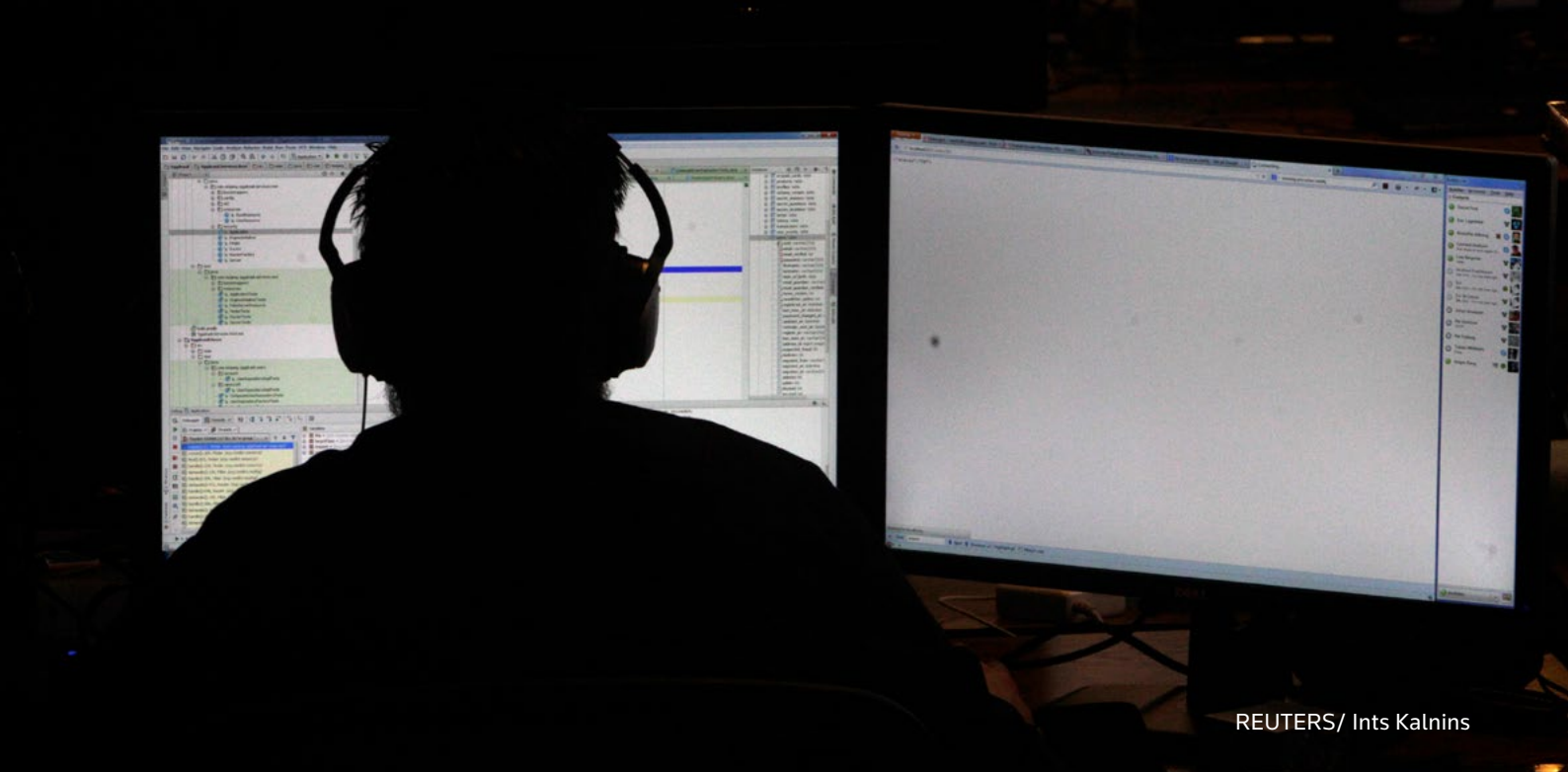


REUTERS/Kacper Pempel

DATA PROTECTION: A GUIDE FOR CHARITIES AND NON-GOVERNMENTAL ORGANISATIONS


[November 2024]



REUTERS/ Ints Kalnins

ACKNOWLEDGMENTS

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



Duncan Turner
Joy Calder
Claire Brown
Ambreen Rasool
Rachel Lawson



Erika Hayes



REUTERS/ Toby Melville

DISCLAIMER

This report is offered for information purposes only. It is not legal advice. Readers are urged to seek advice from qualified legal counsel in relation to their specific circumstances.

We intend the report's contents to be correct and up to date at the time of publication, but we do not guarantee their accuracy or completeness, particularly as circumstances may change after publication. CMS Cameron McKenna Nabarro Olswang LLP and the Thomson Reuters Foundation, accept no liability or responsibility for actions taken or not taken or any losses arising from reliance on this report or any inaccuracies herein.

CMS Cameron McKenna Nabarro Olswang LLP generously provided pro bono research however, the contents of this report should not be taken to reflect the views of the law firms or the lawyers who contributed.



REUTERS/ Kacper Pempel

ABOUT US

The [Thomson Reuters Foundation](#) is the corporate foundation of Thomson Reuters, the global news and information services company. As an independent charity, registered in the UK and the USA, we leverage our media, legal and data-driven expertise to strengthen independent journalism, enable access to the law and promote responsible business. Through news, media development, free legal assistance and data intelligence, we aim to build free, fair and informed societies.

TrustLaw, an initiative of the Thomson Reuters Foundation, is the world's largest pro bono legal network. Working with leading law firms and corporate legal teams, we facilitate free legal support, ground-breaking legal research and resources for non-profits and social enterprises in over 190 countries. By spreading the practice of pro-bono worldwide, TrustLaw wants to strengthen civil society and drive change. If you have ideas for resources we could develop or [legal research projects](#) that would be of assistance after reading this guide, please [contact us](#). If you are a non-profit or social enterprise in need of legal support, you can find out more about the service [here](#) and join [TrustLaw](#) for free.



REUTERS/ Thomas Peter

PREFACE

In today's digital age, the protection of personal data has become a fundamental concern for organisations worldwide. For non-profit organisations in the UK, understanding and complying with the General Data Protection Regulation (GDPR) is essential not only to ensure legal compliance but also to maintain the trust and confidence of the communities they serve.

This guidance report aims to demystify the complexities of GDPR for non-profit organisations, providing clear, actionable insights tailored to the unique challenges and opportunities faced by the sector. Whether you are a small charity or a large non-governmental organisation, this document offers practical advice to help you navigate the intricacies of data protection with confidence and integrity.

We recognise the invaluable contributions that non-profits make to society, and it is our hope that this report will empower you to continue your vital work while safeguarding the personal information of those you serve. By adhering to GDPR principles, you not only ensure compliance but also reinforce your commitment to transparency, accountability, and ethical responsibility.


We extend our gratitude to CMS Cameron McKenna Nabarro Olswang LLP whose insights and expertise were instrumental in developing such a comprehensive and accessible resource.

As you engage with this guidance, we encourage you to reflect on the principles of GDPR not just as regulatory requirements but as opportunities to enhance trust, build stronger relationships, and demonstrate your organisation's dedication to protecting the privacy rights of individuals.

Sincerely,
Carolina Henriquez-Schmitz
Director, TrustLaw

CONTENTS

INTRODUCTION	7
1. WHAT IS DATA PROTECTION?	8
2. THE LEGAL IMPORTANCE OF DATA PROTECTION	11
3. WHAT DO DATA PROTECTION LAWS REQUIRE?	13
4. WHAT PRACTICAL STEPS SHOULD CHARITIES AND NGOS TAKE TO COMPLY WITH THE DATA PROTECTION LAWS?	15
5. KEY QUESTIONS TO ASSIST WITH COMPLIANCE	19
6. FUNDRAISING AND CAMPAIGNS	22
7. CHILDREN'S DATA	25
8. TRANSPARENCY IN HEALTH AND SOCIAL CARE	26
9. USEFUL RESOURCES	27

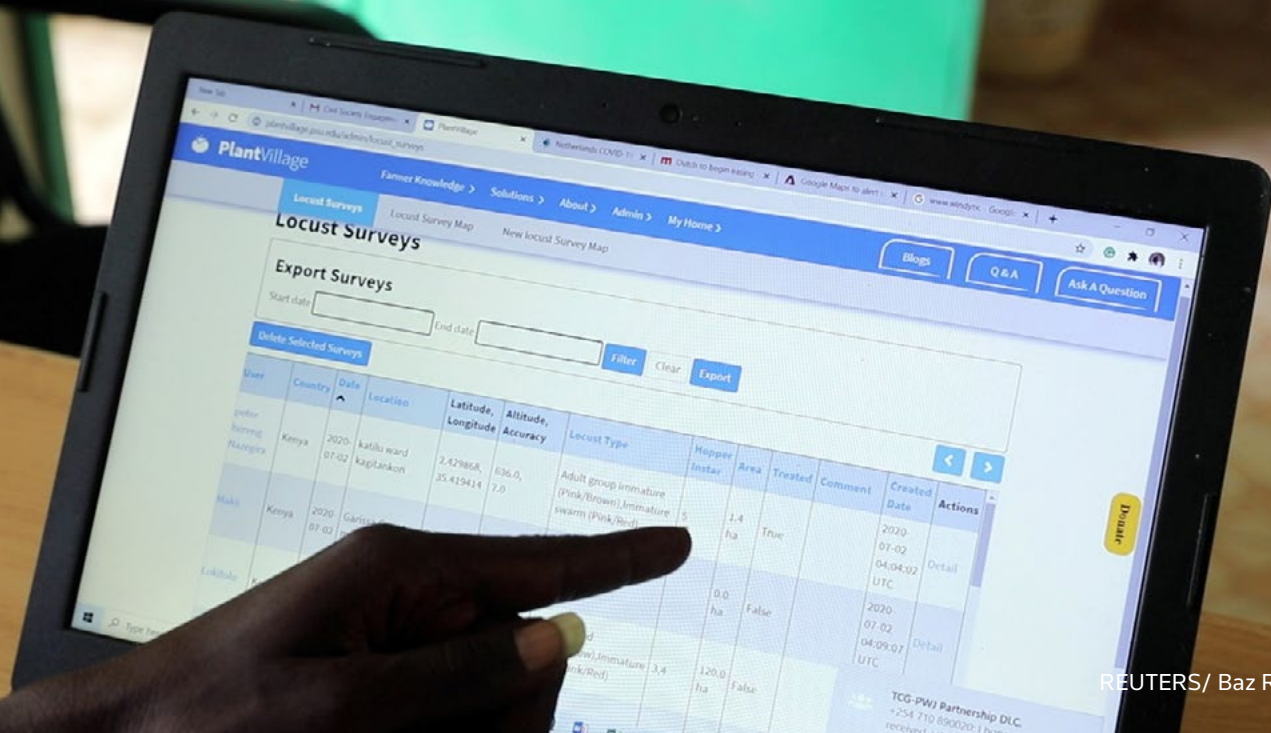


REUTERS/ Nacho Doce

INTRODUCTION

As dealing with personal data has become increasingly central to how modern organisations operate, knowing how to properly protect that data is crucial to meeting the expectations of legislation, regulators, and the public.

This guide provides charities and NGOs with an introduction to the data protection rules that govern the way they collect and use personal data. This guide aims to help charities and NGOs meet their obligations under data protection legislation in the UK but is not intended to be an exhaustive guide and should not be considered a substitute for legal advice.



REUTERS/ Baz Ratner

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 likely include staff, volunteers, donors, suppliers, and users of their services (collectively referred to as **data subjects**).

WHAT LAWS APPLY IN RELATION TO THE COLLECTION AND USE OF PERSONAL DATA BY CHARITIES AND NGOS?

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

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

- the UK General Data Protection Regulation (the **UK 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**).

Charities and NGOs may also wish to be aware of Privacy and Electronic Communications (EC Directive) Regulations 2003 (the **Privacy Regulations**), which 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). The rules regarding use of electronic communications for marketing purposes will apply to communications that promote aims or ideals, as well as those that are part of fundraising activities. This is UK law derived from an EU Directive, as such, these regulations continue to have full effect in the UK.

While the UK GDPR and the EU GDPR are broadly similar, these are independently regulated, and we may see divergence in the future.

The EU GDPR has effect beyond the EU's borders, so the EU GDPR may continue to apply to UK organisations with a presence in the EU, or who offer goods or services to data subjects in the EU. Such organisations may therefore find themselves subject to dual data protection regulatory regimes under the UK GDPR and the EU GDPR.

There is more information about the geographic reach of the EU GDPR in the European Data Protection Board's [guidelines](#).

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), and covers:

- Data that clearly relates to a person – such as their name or email address; and
- Data that by itself does not identify a person, but which could identify a person when combined with other information that an NGO or charity holds. For example, an NGO or charity may hold records that do not identify a person by name but have 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.

WHAT ACTIVITIES ARE REGULATED BY DATA PROTECTION LAWS AND WHO REGULATES THIS?

Data Protection Laws regulate the "processing" of personal data. Processing covers a wide range of activities that a charity or NGO may do with data, including its collection, storage, use, and destruction.

The Information Commissioner's Office (the **ICO**) upholds the Data Protection Laws through regulation and enforcement (by investigating complaints, issuing fines, conducting audits etc.), providing guidance and advice to help organisations understand their obligations, and running educational campaigns and resources to allow the public to understand their rights under the Data Protection Laws. In addition to the ICO's enforcement powers, ICO guidance is considered best practice and adherence can be used to demonstrate to courts or tribunals an organisation's efforts to comply with Data Protection Laws.

WHO DO DATA PROTECTION LAWS APPLY TO?

Data Protection Laws apply to NGOs and charities established in the UK.

However, NGOs and charities based outside the UK are also caught by UK GDPR to the extent they process personal data relating to UK data subjects.

WHAT ARE THE PRINCIPLES AT THE HEART OF DATA PROTECTION?

There are six principles NGOs and charities must follow when processing personal data under the UK GDPR.

1. Processing must be done **fairly, lawfully and in a transparent manner**. This means:
 - Being transparent with 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; and
 - Having one of the six available lawful basis which allows you to process the personal data of data subjects. For example, where the NGO or charity has a legitimate interest in processing the personal data, or has obtained the consent of the data subject. The ICO has a [guide](#) that provides more information about the available grounds for lawful basis.

Privacy notices provide a good way to communicate this information (see section 4 for further information)

The ICO has produced [guidance on what privacy information should be provided to data subjects](#).

The processing of **special categories of personal data** (such as data about a person's racial or ethnic origins, political opinions, sexuality etc.) is subject to further conditions due to the sensitive nature of the data. The ICO has produced [guidance on the conditions for processing special category personal data](#).

2. Personal data must be acquired for a **clear and specified purpose**. NGOs and charities must use personal data in the way they informed data subjects it would be used.
3. Personal data collected must be **adequate, relevant, and not excessive**. NGOs and charities should be collecting personal data for a specific purpose(s), and 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**. NGOs and charities should take reasonable steps to correct or erase any personal data they discover to be incorrect or misleading as soon as possible.
5. Personal data should be retained for **no longer than necessary**. NGOs and charities should delete personal data when it is no longer required.
6. Personal data must be kept **secure**. NGOs and charities should ensure they have robust physical and technical security measures to protect the personal data which is proportionate to the risk (e.g. more sensitive data will require more protection).

2. THE LEGAL IMPORTANCE OF DATA PROTECTION

Charities and NGOs often handle large amounts of highly sensitive personal data. If you fail to protect it properly, and do not process it in accordance with the relevant Data Protection Laws, you might expose your organisation to potentially serious legal, operational, and reputational risks. Data protection compliance means good data management which can, in turn, save your organisation time, effort, and money. Further, demonstrating proper protection of data subjects' personal data will allow you to develop and maintain trust and confidence in your organisation.

Data protection should therefore form an integral part of your risk management and operational strategies, and it is important to ensure that personal data is handled securely, and in accordance with the Data Protection Laws.

WHAT ARE THE RISKS OF GETTING IT WRONG?

- **Fines** - Breaching the UK GDPR puts your organisation at risk of receiving significant monetary penalties. Regulators can impose fines for serious breaches of up to £17.5 million or 4% of an organisation's global turnover, whichever is higher.
- **Legal Actions** – Your organisation may face legal actions for breaches, this will usually be a data subject(s) enforcing their rights and/or seeking compensation following breaches, but there is also the potential for criminal charges.

- **Financial Costs** – In addition to fines, financial costs could be incurred when having to pay to; rectify a data breach, compensate those impacted, and implement the necessary data protection measures which should have been in place.
- **Reputational Damage** - Public confidence and trust in your organisation will likely reduce, this could impact donor support, partnerships, and service users.
- **Operational Disruption** – The loss of data or major works to rectify the position of data protection processes could disrupt organisational work and prevent ongoing projects from progressing.

Some charities have come under criticism for their failure to comply with Data Protection Laws, and the ICO have highlighted various examples where they have taken action to ensure compliance.

FUNDRAISING

The ICO lists three ways charities have been improperly handling data 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, guidance is available on the ICO's [website](#).

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. Not screening their database of phone numbers against the TPS and subsequently targeting people who have opted out of marketing calls.



REUTERS/ Jose Manuel Ribeiro

3. WHAT DO DATA PROTECTION LAWS REQUIRE?

There are key obligations created by the Data Protection Laws that NGOs and charities should be aware of.

- **Accountability** - NGOs and charities cannot simply 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 UK GDPR accountability principle on their [website](#).

- **Consent** - Under the UK GDPR, “consent” means any **freely given, specific, informed, and unambiguous** indication of a person’s wishes by which they agree to the processing of their data, through a **statement or clear affirmative action**.

Individuals must not feel forced to consent to their data being used by you or have their consent bundled as a condition of service. They must also be able to withdraw their consent at any time.

An individual must consent to the specific way their data will be processed, separate consents should be obtained for distinct processing activities.

There should be a positive indication that an individual has consented. Consent is not the default, so methods such as silence, inaction, or a pre-ticked opt-in box will not constitute valid consent.

The ICO provides further [guidance](#) on what constitutes valid consent on their website.

Privacy-by-Design – NGOs and charities might be required to conduct a data protection impact assessment (DPIA) in certain circumstances to ensure privacy is factored into new initiatives. DPIAs are a systematic process intended to allow organisations to effectively identify a projects data protection risks and assess how these risks can best be mitigated.

The ICO has [guidance](#) to help you determine whether you should conduct a data protection impact assessment.

- **Data Protection Officers (DPO)** - A DPO is an independent data protection expert whose duties include monitoring and advising on internal compliance with Data Protection Laws and data protection strategies, being a point of contact for the ICO and data subjects and running training and awareness events for staff.

There are certain circumstances where 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.

The ICO offers a [set of questions](#) which will help you determine if you require a DPO.

- **Personal Data Definition** - NGOs and charities have data protection obligations in relation to a wide variety of data.

The UK GDPR allows for a broad range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people, for example, information such as an online identifier (like an IP address) can be personal data.



REUTERS/ Jessica Orellana

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

1. **Have Appropriate Training in Place** – Ensure people in your charity or NGO are aware of Data Protection Laws and the obligations relating to the processing of personal data which they impose.

If you have created new internal policies to help ensure data protection compliance within your organisation, ensure 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. **Implement a Data Retention Policy** – Charities and NGOs should know who their data subjects are, where the data came from, how and why the data was collected, and how it is used (including who it is shared with.)

A Data Retention Policy can be an effective way of standardising how information is retained from the point of creation through to the data being destroyed. This generally includes the types of information held, the reason and use for the data being held, and how long the data is intended to be retained.

- 3. Make sure you have a Legal Basis for Processing Data** – Ensure you have a legal basis for processing information and retain documentation to record the type of personal data your organisation uses and the legal basis for that use.

Broadly, the available legal basis are:

- **Consent** – where a data subject has given clear consent for their data to be processed for a specific purpose;
- **Legitimate interest** – where processing is necessary for your legitimate interests (such as fraud prevention or marketing) and your legitimate interests are not overridden by the impact on the data subject;
- **Contract** – where processing is necessary for a contract you have with a data subject, or because they have asked you to take specific steps before entering into a contract;
- **Legal obligation** – where processing is necessary to comply with a legal obligation;
- **Vital interests** – where processing is necessary to protect someone’s life; and
- **Public task** – where processing is necessary for a public interest task or for an official function with a clear basis in law.

If you think any of the above lawful basis may apply to your processing activity, you should consult the ICO [guidance](#) on lawful basis to learn more.

- 4. Consider how you will obtain consent** - If your legal basis for processing personal data is ‘consent’, you should review your consent mechanism and ensure it meets the criteria described in the UK GDPR (i.e. freely given, specific, informed, and unambiguous). (See section 3 above for further information about consent)

The ICO has further [guidance](#) and a checklist on consent on its website.

- 5. Have Appropriate Contractual Arrangements in Place** - The Data Protection Laws require that charities and NGOs have effective contract documentation in place for the processing or sharing of personal data with other organisations (including where you transfer data to a supplier so they can provide you with a service).

If you share data with other organisations, you must ensure a written agreement is in place. Existing agreements should incorporate the necessary processing provisions.

The ICO explains what you must include in such agreements in order to comply with the Data Protection Laws on its [website](#).

In addition, personal data relating to UK data subjects may only be transferred outside of the UK when done in compliance with the specific conditions set out in the Data Protection Laws.

The ICO has [guidance](#) on international transfers of data.

- 6. Ensure transparency regarding 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 information (a privacy notice provides data subjects with information about how their information will be gathered and used, as well as the legal grounds for doing so). Ensure a privacy notice is in place and review existing privacy notices to ensure they meet the requirements of the Data Protection Laws, update them, and show them to data subjects.

The ICO has produced a helpful [guide on privacy notices](#) on their website.

- 7. Have a Data Subject Access Request Procedure** - Data subjects have a right to request access to their personal data that your organisation holds. In preparation for receiving these types of requests, you should bear in mind the following:

- *Fees* - Fees cannot be charged for data subject access requests unless the 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 the request being received (although an extension can be requested in certain circumstances).

You should ensure relevant policies and procedures are in place and up to date to allow data subject access requests to be responded to in line with the above requirements.

The ICO has prepared [guidance for responding to data access requests](#).

- 8. Be Prepared to give effect to Data Subject Rights** - The Data Protection Laws provide a number of rights for data subjects. For example, data subjects may request a copy of the personal data that an NGO or charity holds about them, or request they delete their personal data. Preparing to respond to these rights being exercised is important to ensure timely and appropriate responses in line with the requirements and timelines of the Data Protection Laws.

The ICO explains these rights in more detail and provides checklists in its [guide to individual rights](#).

- 9. Have measures to prevent Data Breaches** - Charities and NGOs should implement appropriate security measures to ensure data security and account for risk (with more sensitive data being protected with more robust security measures).

The ICO has a [guide on data security](#) with further information.

- 10. Prepare for Data Breaches.** Organisations have an obligation to inform regulators (and in some circumstances, data subjects) about data breaches. Ensure you have a response plan and the means necessary to detect, investigate, and report breaches within 72 hours of becoming aware of any data breach.

To prepare, you can use the ICO's [checklist on data breaches](#).

- 11. Know when to conduct a Data Protection Impact Assessment** – If you are thinking of undertaking a project that processes personal data, data protection should be considered at the outset. Conducting a data protection impact assessment will help you to identify and minimise any data protection risks. (See Section 3 for further information about data protection impact assessments)

Ensure you know when to carry out a DPIA, by reviewing the ICO's [guidance on DPIAs](#).

- 12. Consider if it is necessary to appoint a Data Protection Officer (DPO)** – You may be required to appoint a DPO (see Section 3 for further information about data protection officers).

The [ICO's guidance](#) can be used to help your organisation to determine if a DPO should be appointed.

- 13. Treat Children as Vulnerable Persons** - If you are collecting data directly from children under the age of 13, make sure it is done fairly. Consider whether systems should be implemented to verify data subjects' ages or whether privacy notices should be made clearer, so children fully understand what information is processed about them and why (see section 7 for more detail).

More [guidance](#) on the issues to be considered when processing children's personal data is available on the ICO's website.

- 14. 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 also fall under the jurisdiction of another data protection supervisory authority.

Charities based in England and Wales may also have data protection breaches reported to the Charity Commission as a "serious incident". A "serious incident" is an adverse event (whether actual or alleged) which results in or risks significant loss, damage, or harm to a charity's assets, beneficiaries, or reputation.

Further information can be found here: [How to report a serious incident in your charity - GOV.UK \(www.gov.uk\)](#).

Charities based in Scotland should follow the Scottish Charity Regulator (OSCR) "Raise a concern" procedure.

Further information can be found here: [2016-03-15 guidance-for-notifiable-events_web-version.pdf \(oscr.org.uk\)](#)

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?**
 - i. e.g. employees, volunteers, service users, donors etc.
- b. **What types of personal data do you collect?**
 - i. e.g. name, address, date of birth, payment details etc.
 - ii. See Section 4.2 above.
- c. **Do you collect any special categories of personal data?**
 - i. 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?**
 - i. See Section 4.13 above.
- e. **How do you collect personal data?**
 - i. e.g. directly from the data subject, from a third party (like a social worker, school etc.) or from a relative or guardian of the data subject?
- f. **Do you use/operate CCTV?**
 - i. CCTV footage may constitute personal data where an individual is identifiable, the same considerations will apply to this footage as other forms of personal data.
 - ii. The [ICO CCTV checklist](#) can assist in assessing a CCTV system.
- g. **Can you minimise the personal data you collect?**
 - i. 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?**
 - i. See Section 4.3 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?**
 - i. 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?**
 - i. See Section 4.6 above.
- b. **Has the data subject been told what purposes you will be using their personal data for?**
- c. **Do you have an internal privacy policy for staff?**
 - i. e.g. employees, contractors, and volunteers
- d. **If applicable, do you have signs/notices informing data subjects that you will be collecting CCTV data?**
- e. **Do you rely on consent to process personal data? If so, how do you record consent? Does your process for collecting consent comply with the requirements under the UK GDPR? Are data subjects told they can withdraw their consent at any time? And do you have a process for dealing with withdrawals of consent?**
 - i. See Section 4.4 above.
- f. **Do you use personal data for marketing communications? Do you have the appropriate consent 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?**
 - i. See Section 4.9 above.

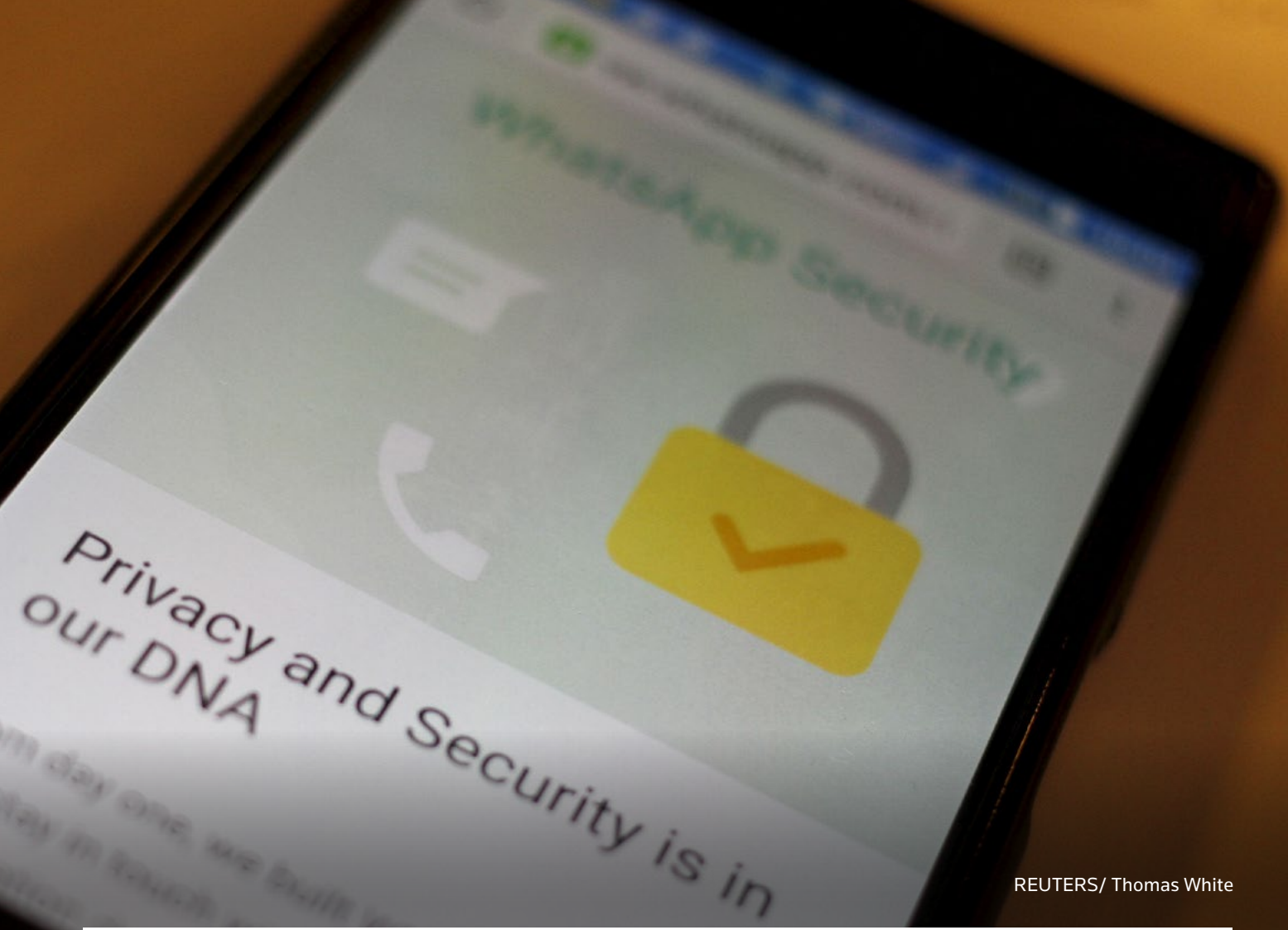
- b. **How frequently do you review and test the security measures you have in place? How is this documented?**
- c. **Do you have internal policies informing staff about how to keep personal data secure?**
- d. **Do you provide training for staff to inform them of good practices to keep personal data secure?**
 - i. 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?**
 - i. See Section 4.5 above.
- c. **Do you transfer personal data outside the UK? For example, to servers hosted outside of the UK? If so, how do you ensure compliance with the rules on overseas transfers of data?**
 - i. See Section 4.5 above
- d. **Whose responsibility is it to respond to requests from data subjects?**
 - i. See Section 4.7 and 4.8 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?**



REUTERS/ Thomas White

6. FUNDRAISING AND CAMPAIGNS

Data Protection Laws include rules that apply to the marketing activities of charities and NGOs.

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.
2. **Third party lists** – Be cautious when purchasing lists of prospective donors from third parties for emails or marketing calls. These third parties must demonstrate they have lawfully obtained the data, and that it 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. Unsolicited marketing calls** - Charities and NGOs should **NOT** make unsolicited marketing calls to:
 - a. an individual or 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/CTPS** - TPS and CTPS are central registers of individuals and organisations who have opted out of receiving marketing calls. The TPS list contains details of individuals, partnerships (England and Wales only), and sole traders who have opted out of receiving marketing calls, and the CTPS contains details of organisations (limited companies, public limited companies and Scottish partnerships) who have opted out of receiving marketing calls. Contacting individuals or organisations listed on TPS/CTPS 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), you must comply with Data Protection Laws. In particular, the individual should be aware you have their number, plan to use it for marketing purposes, and consented to such contact prior to receiving the call.

At the start of the call, 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. Adhere to the individuals' instructions** - If someone asks not to be contacted, ensure that they are added to the suppression list and not contacted in future. If they ask to be contacted by email, do that instead.

EMAIL MARKETING

- 1. Consent** - Generally, you cannot send marketing emails without prior opt-in consent of the individual. There are limited exceptions to the opt-in consent requirement under the Privacy Regulations. You should check whether these apply.
- 2. Opt-outs** - Individuals have the right to ask you to stop sending them marketing. If they do this, ensure their details are added to the suppression list.

- 3. Compliance with 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.

MARKETING CONSENT

Marketing consents must be freely given, specific, informed, unambiguous, and involve a clear affirmative action. You may wish to review existing marketing consents and your consent mechanisms to verify they meet the standard required under Data Protection Laws.

PROFILING

Data Protection Laws contain specific rules around profiling individuals, if the profiling involves automated processing of personal data (i.e. without human intervention), and this has legal effects or significantly affects the individual. If you are considering activities involving profiling individuals to ascertain their financial status or propensity to donate, you may wish to review the [ICO guidance](#) on automated decision making (including profiling)

MORE INFORMATION

Direct marketing includes any promotion of an organisations aims or ideals, and is not restricted to fundraising purposes. This encompasses various activities which charities or NGOs may wish to promote such as encouraging people to take direct action through contacting a member of Parliament, signing a petition, voting a certain way, attending an event, etc.

The ICO has [further information](#) about electronic and telephone marketing.



REUTERS/ Louisa Gouliamaki

7. CHILDREN'S DATA

The ICO has introduced a statutory [code of practice](#) on age-appropriate design which requires specific protections to be built into websites and apps that may be used by children (the **Age Appropriate Design Code**, or the **Children's Code**).

The Children's Code sets out 15 standards organisations should meet to protect children's privacy, including the following:

- The **child's best interests** should be considered when designing and developing online services likely to be accessed by a child.
- **Data protection impact assessments** should be carried out to assess and mitigate risks.
- Information must be **concise, prominent, and in clear language suited to the age of the child** and additional specific "bite-sized" information should be provided at appropriate points.
- Children's data should not be used in ways shown to be **detrimental to their wellbeing**, or against industry codes, regulatory provisions, or government advice.
- Settings should be **"high privacy" by default** unless there is a compelling reason not to.
- Where there are **parental controls**, children should be given age-appropriate information about this.
- **Profiling options should be switched off by default** (unless there is a compelling reason not to), and profiling should only be allowed if there are appropriate measures to protect children from any harmful effects.
- **Nudge techniques** (features designed to channel users towards specific paths or decision-making) should not be used to lead or encourage children to provide unnecessary personal data or turn off privacy protections.

These standards focus on ensuring the child understands how their personal information being processed, and can provide (and withdraw) consent to such processing. Importantly, the rights belong to the child (not a parent or guardian), even if they are too young to understand the implications.

The ICO has provided further information about the code on its [website](#).



REUTERS/ Susana Vera

8. TRANSPARENCY IN HEALTH AND SOCIAL CARE

The ICO has [guidance](#) on implementing transparency principles in a health and social care setting, including research and planning in connection with these sectors. The sensitive data being processed in this sector makes it paramount to implement good practice when handling personal information, which will in turn help to maintain patient trust.

Health data is a form of special category data and will therefore be subject to stricter conditions when processing. More information on the conditions for processing are available on the ICO's [website](#).

The guidance provides details of how to effectively provide, and assess materials which are intended to inform data subjects of how their data is used in a healthcare setting. Below are the key considerations the guidance encourages organisations to consider. The transparency principle and requirements generally are discussed at section 4 above.

1. CONSIDERING THE FORM OF COMMUNICATION

Transparency information must be easy to access. Common methods for providing such information include posters, letters, emails, texts, social media, advertising campaigns, and pop-ups and just-in-time notifications.

While one to one communication methods, such as letters or emails, can be effective, it is important to consider the impact of such methods on individuals. For example, sending an in-depth explanation of your privacy policy to someone without the capacity to understand such information would be inappropriate and potentially harmful.

2. PRIORITISING INFORMATION

The guidance encourages a layered approach to transparency which cultivates awareness at all levels of patient involvement. This could include e.g. a poster with some basic details about how you use personal data and where they can access a more detailed privacy notice which provides more in-depth information.

Communications should use clear, plain, and accessible language to prioritise key information, such as:

- An overview of how personal data is used and the purpose for such use;
- Choices or actions available to people regarding how you use personal data; and
- Guidance on where to find more detailed information.

3. WORKING WITH OTHER ORGANISATIONS

When working with other organisations to deliver health and social care services, privacy materials should be “joined up” in a logical way which considers how users will interact with the different services.

9. USEFUL RESOURCES

For additional resources relating to data protection and further information on complying with Data Protection Laws, you may wish to consult:

[Information Commissioner’s Office](#) website, which has:

- General guide to [data protection](#).
- Advice on topics such as [direct marketing](#) and [CCTV](#).
- [A self-assessment toolkit](#) for small and medium enterprises.
- A booking service to [request an advisory visit](#) to your organisation with a short follow up report.
- An advice service by phone on 0303 123 1113 or email icocasework@ico.org.uk

The [Fundraising Regulator Code of Practice](#), which reflects key aspects of the Data Protection Laws.

