CAMPAIGNING LEGAL GUIDE: DATA PRIVACY

2019

REUTERS/KACPER PEMPEL

Bates Wells

THOMSON REUTERS FOUNDATION

CAMPAIGN BOOTCAMP

ACKNOWLEDGEMENTS

The Thomson Reuters Foundation is extremely grateful to the following authors of this Guide. This Guide would not have been possible without their expertise, time and commitment to pro bono work.

Bates Wells

Mark Abbott is an associate at Bates Wells and specialises in providing data privacy, election law and charity law advice to charities, issue-based campaigners, political parties, businesses and non-profits. His advice on information law includes GDPR compliance and "direct marketing" rules as they apply to the fundraising and advocacy efforts of non-profits.

DISCLAIMER

This Report and the information it contains is provided for general information purposes only. It has been prepared as a work of legal research only and does not represent legal advice in respect of the laws of the United Kingdom. It does not purport to be complete or to apply to any particular factual or legal circumstances. It does not constitute and must not be relied or acted upon as legal advice or create an attorney-client relationship with any person or entity. Neither the Thomson Reuters Foundation nor any other contributor to this Report, accepts responsibility for losses that may arise from reliance upon the information contained in this Report or any inaccuracies herein, including changes in the law since the research was finalized in 2019. Legal advice should be obtained from legal counsel qualified in the relevant jurisdiction(s) when dealing with specific circumstances. Neither the Thomson Reuters Foundation not any other contributor to this Report is holding itself, himself or herself out as being qualified to provide legal advice in respect of any jurisdiction as a result of his or her participation in or contribution to this Report.

ABOUT US

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, connecting the best law firms and corporate legal teams around the world with high-impact NGOs and social enterprises working to create social and environmental change. We produce groundbreaking legal research and offer innovative training courses worldwide. Through TrustLaw, over 120,000 lawyers offer their time and knowledge to help organisations achieve their social mission for free. This means NGOs and social enterprises can focus on their impact instead of spending vital resources on legal support. TrustLaw's success is built on the generosity and commitment of the legal teams who volunteer their skills to support the NGOs and social enterprises at the frontlines of social change. By facilitating free legal assistance and fostering connections between the legal and development communities we have made a huge impact globally.

We have supported grassroots organisations to employ their first staff members, helped vulnerable women access loans to start their first businesses and brought renewable energy lighting to slums. Free legal assistance on these small projects has had a big impact on local communities working to overcome poverty and discrimination. At a global scale, we have supported legal reform activities to protect the rights of millions of domestic workers, changed legislation to support victims of violence, produced guides to protect people who experience street harassment, and crafted tools to support the prosecution of trafficking offenders.

Legal research reports and other TrustLaw publications are legal resources that take an in-depth look at a legal issue in a number of countries. This may be in the form of a comparative analysis of laws in different countries, or a legal landscape analysis. These resources aim to help TrustLaw members advocate for legal reform, inform policy activities or propose legal amendments.

Our resource library can be found on the TrustLaw homepage at www.trust.org.

ABOUT BATES WELLS

Bates Wells is a leading law firm for charities and campaigning organisations. The firm's specialist politics, elections and campaigning law team helps political parties, candidates, donors, charities and issue-based campaigners navigate the complex regulatory environment that can be relevant to their electoral and policy goals. The multi-disciplinary team works across all areas of campaigning law, from election and referendum law to campaign finance, transparency of lobbying, data privacy, charity law, public law, strategic litigation, advertising and reputation-management.

Bates Wells regularly advises on the biggest political issues of our time, including Brexit, where it advised Britain Stronger in Europe – the official Remain campaign. The firm is rated for electoral law advice in both Chambers and Legal 500, which has referred to it as an "incomparably excellent' team, which 'uniquely understands the broader issues'.

For more information, please contact Simon Steeden at s.steeden@bateswells.com. Simon is a partner in the charity and social enterprise team at Bates Wells and co-leads its specialist political and campaigning law team.

ABOUT CAMPAIGN BOOTCAMP

Campaign Bootcamp is a charity dedicated to ensuring that people most impacted by injustice are leading campaigns that affect their lives, from better housing to fairer treatment of migrants and LGBTQ+ rights. Our graduates wage important, successful campaigns, testify before Parliament, appear in the national and international press, organise demonstrations, get elected to local government, and change laws.

We do this work because we've found that today it's far too hard for ordinary people, especially those in marginalised communities, to challenge those in power. Because of this, injustices persist and millions of people do not live happy, safe and fulfilled lives.

Our programmes are designed to be accessible to anyone who wants to make change happen. If you want to learn how to run powerful campaigns go to www.campaignbootcamp.org to find out more about our training, including how to apply. You can also check out our range of stories, free resources, and our blog about our programmes and what our graduates get up to outside of camp.

Campaign Bootcamp Residential is a week-long training programme that supports you to develop the skills, confidence, and community to run powerful campaigns.

The training brings together 35 budding campaigners and activists from across the country (and sometimes further afield) to learn and build a community together.

In the course of a week, Campaign Bootcamp will take you on a journey through planning and running an effective campaign, giving you space each day to work out how what you have learnt applies to the work that you are doing. Each day has a different theme reflecting a different part of your campaign. By the end of the week, you will come out with a campaign strategy that you can take forward to make change happen. To gain the skills, community and confidence you need to run your campaign at the Campaign Bootcamp residential, apply today at www.campaignbootcamp.org/apply.

CAMPAIGN BOOTCAMP

TABLE OF CONTENTS

FOREWORD

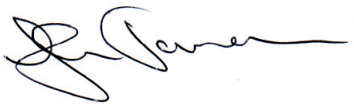
Many of the organisations TrustLaw supports engage in campaigning activities, community engagement and advocacy, with the aim of highlighting and solving social problems and encouraging systemic change.

The closing space for civil society means that campaigners are under increasing pressure to run campaigns for social change that are not only politically effective but are also run in compliance with the law. Campaigners do not always have the time or expertise to analyse and understand a complex and evolving legal landscape and, as a result, may unwittingly break the law, restrict their activities unnecessarily through defensive decision making, or be discouraged from engaging at all.

In collaboration with Bates Wells and Campaign Bootcamp, TrustLaw's goal is to support the development of a resilient and informed campaigning community by publishing this series of legal guides for campaigning and advocacy organisations in the United Kingdom.

The guides offer campaigners advice and tips on how to comply with the laws that apply to their day-to-day activities. These guides aim to arm campaigners with the legal information needed to navigate issues including: political activities, election and lobbying laws; defamation and campaigns that target companies; hacktivism and shareholder activism; the right to protest and laws relating to marches, assemblies and police powers; using social media and online campaigns; data protection and direct marketing.

We hope that these guides will ultimately empower campaigners to act with confidence and achieve the positive outcomes they seek.



Glen Tarman
Director of TrustLaw
Thomson Reuters Foundation

DATA PRIVACY

REUTERS/STEFAN WERMUTH

DATA PRIVACY

1. Whether you wanted to or not, you will probably have heard a tremendous amount recently about the General Data Protection Regulation (GDPR). Other laws which have been less widely publicised but should be mentioned at the same time are the Data Protection Act 2018 (the DPA), and the Privacy and Electronic Communications Regulations 2003 (PECR).

2. These laws are very relevant to campaigning and advocacy activity. It would be difficult to campaign properly without processing people's personal details in some way and so coming within the scope of the rules. At a minimum, the campaigning organisation will employ staff. It will also want to maintain a database of its supporters (including their names and contact details), which it can use to update them on the causes that they are supporting and the success of the campaign; to persuade them to involve other people in the campaign; and to arrange events or volunteering opportunities with them. Because, by definition, advocacy involves engaging with people who are not already supporters of the cause, campaigning bodies often acquire and maintain lists of individuals who are not already engaged with them, and use this to knock on their door or telephone them, for example. Additionally, organisations (either directly or through third parties) often now undertake increasingly sophisticated work to analyse their supporters and potential supporters, to identify potential characteristics of their intended audiences, and to tailor their campaigning message in a way which is likely to achieve a greater impact.

3. **What laws apply?**

   As mentioned above, at the moment, in the UK there is:

   (a) **GDPR** and the **DPA**. GDPR is the main law regulating the processing of personal data. It applies in most circumstances (except where a person is engaged in personal and household activities, for example). The DPA then sits on top of GDPR and fills "gaps" in it. For example, it creates rules where the European Union does not have competence to create law. It also creates rules where GDPR has given EU member states discretion to decide the rule themselves – for example, the UK has decided that children can consent to receive certain online services from the age of 13, instead of 16. The DPA also contains a regime for processing by law enforcement agencies (implementing a separate EU directive), and information about the regulator, the Information Commissioner's Office (ICO). You therefore need to look at the two laws in conjunction with each other.

   (b) **PECR**. This is a separate piece of law regulating electronic communications. For present purposes, the key point to note is that it requires you to gain consent to "direct marketing" to individuals by SMS or email. For live telephone calls, it

requires you to check whether the individual is registered with the Telephone Preference Service (**TPS**). If they are, you can only phone them for "direct marketing" purposes if the person has indicated that they do not (for the time being) object to being phoned. PECR also contains rules about cookies and similar technologies (which generally require consent). Confusingly, the definition of consent is found in GDPR. The European Union is in the process of agreeing a new law which covers this area – the e-Privacy Regulation (**ePR**), which was supposed to come into force alongside GDPR. At the time of writing it is in draft form only – but organisations should stay abreast of developments.

The UK is in the process of negotiating its exit from the European Union, which indicates that European Union regulations (such as GDPR and ePR) will at some point no longe be binding on the UK. However, it is likely that the UK will wish to retain a similar high standard of data privacy law, to facilitate easier cross-border transfers of personal data. The landscape will continue to change (for example, GDPR allows for the ICO and others to prepare codes of conduct to assist in compliance).

Public bodies can have separate obligations (and are not covered in detail in this report).

In short, it can all be something of a quagmire. This section explains some of the key principles about the application of these rules, flagging areas that your organisation should be considering in the context of campaigning activity, and key situations in which it may be appropriate to ask for legal advice. Please note that, at the time of writing, the ICO is conducting an investigation into the use of personal data for political purposes; and is consulting on a new "framework code" of guidance on political campaigning activity (referred to in the "further reading" section below) which organisations should also consider.

4. **Does GDPR apply?**

4.1 First, you should consider whether GDPR applies to your processing at all. If it does not, this will significantly lessen the burden of compliance (but you should consider whether you should adopt similar standards anyway, in light of (i) reputational considerations; and (ii) if you operate internationally, other local laws).

4.2 Are you processing personal data?

GDPR applies to the "processing" of "personal data".

For all intents and purposes, anything that you can do with data is "processing" it, including storing it and deleting it.

In turn, GDPR provides that personal data is information relating to:

(a) A living individual;

(b) Who can be identified, directly or indirectly.

It gives examples of not only a person's name, but also an ID number, location data, online identifier, or other factors relating to a person's physical, physiological, genetic, mental, economic, cultural or social identity. To resolve this, you should therefore work out whether it is possible for anyone to identify a person (for example, by singling them out).

In practical terms this also means you should consider the benefits of anonymisation. Truly anonymous data (where no person is identifiable) is not subject to GDPR, and so using it is considerably more straight-forward. For example, if you are looking to analyse trends at a village-by-village or town-by-town level, is it possible to delete the names of the relevant individuals, and other data which might identify them, from your data-set and only use the remaining, anonymous information? Doing this may be time-consuming, but this should be weighed up against the time and cost of ensuring compliance with the data protection regime, and potential penalties (including fines) for not being compliant.

GDPR also introduces a half-way house, "pseudonymisation", where personal data "can no longer be attributed to a specific [person] without the use of additional information [which is] kept separately and is subject to technical and organisational measures" to ensure that no-one is identified. Pseudonymised data is still subject to GDPR, but there is a lesser burden of compliance in some circumstances.

4.3 Are you within the scope of GDPR?

Even where you are processing personal data, GDPR only applies where personal data:

(a) Is processed by automated means (for example, you use a computer); or

(b) Forms part of, or is intended to form part of, a "filing system". That is, where personal data is accessible on the basis of specific criteria. For example, a rolodex or address book of people sorted alphabetically.

Admittedly, in the 21st Century this will catch most uses of personal details. However, ad-hoc, manuscript notes about a person, or a filing system which contains personal data but not in an organised manner, for example, might not be within scope, depending on how it is collected and used. You should take legal advice if it is not clear and you may wish to benefit from this (for example, if you process significant amounts of manuscript data).

As mentioned above, GDPR does not apply in the context of personal and household activities. It also does not apply to areas outside of the scope of EU law, and law enforcement processing, which are subject to separate regimes.

There are also a number of exemptions from parts of GDPR, including in the DPA - which are not fully addressed here.

4.4 What role do you fulfil?

GDPR specifies two different categories of relationship which a person or body may have with personal data, and places different obligations on each.

(a) A **controller** is a person or body which determines the purposes for which the personal data is being processed, and the means by which it is processed. The majority of obligations in GDPR fall on controllers.

(b) A **processor** is a person or body which processes personal data on behalf of the controller – such as a fulfilment house or website server hosting provider. Some obligations are placed on

processors directly, such as keeping records of processing, appointing a Data Protection Officer if needed, and / or keeping data securely.

It is a legal requirement that a controller and processor have an agreement in place between them, containing certain prescribed information and placing obligations on the processor.

This is particularly relevant if you are running a campaign and using suppliers to process information on your behalf. If you have agreements, but they were put in place before GDPR came into effect (in May 2018) you will probably need to review and update them.

4.5 Unhelpfully, as may be apparent from the above, the distinction can also be incredibly difficult to apply in real life. Modern transactions rarely involve (i) an organisation which is completely in control; and (ii) an organisation which is simply acting on instructions. Company A will generally use Company B to do something because Company B has expertise in a particular area (and so will input into the manner in which personal data is processed). Company B will often, in turn, use Company C to provide services to it to help it to fulfil its contract with Company A (which leads to the concept of a 'sub-processor'). Or perhaps Company A and Company B will use the same data for different purposes, but also help each other to fulfil the other's purposes.

4.6 The ICO has published detailed guidance on the subject, seeking to address this issue in the context of GDPR. Among other things, the guidance acknowledges that processors can still make important decisions in relation to personal data, without taking on the mantle of a controller. For example, it considers that processors can decide:

(a) How to store personal data;

(b) What IT systems or other methods to use to collect personal data; and/or

(c) The detail of the security measures to protect the personal data.

(d) How it will transfer personal data from one organisation to another;

(e) How it will ensure it adheres to a schedule setting out how long particular personal data is kept;

(f) How it will retrieve personal data about particular people; and

(g) How it will delete or dispose of data.

On the other hand, areas which the ICO considers are reserved for the controller include:

(h) Which individuals to collect data about;

(i) The legal basis for using the data;

(j) What the data is used for;

(k) What to tell people about the processing;

(l) How to respond when people look to exercise their rights under data privacy law;

(m) How long to keep the data and whether to amend it in a non-routine way;

(n) Whether to disclose the data, and if so, who to; and

(o) Which items of personal data to collect.

4.7 Taking this guidance into account, it seems like a fair assumption that an organisation which has decided to engage in campaigning activity for its own purposes is a controller. However, to avoid falling foul of data rules, entities should also consider the status of the other organisations who they work with, and properly documenting the relationship between them.

4.8 Are you in territorial scope?

(a) GDPR applies to processing "in the context of the activities of an establishment of a controller or a processor in the [European Union]". This has historically been quite broadly defined. For this purpose, it does not matter whether the data is processed inside or outside of Europe, or whether the individuals live in Europe or not.

(b) Even if you (a controller or processor) are not established in the European Union, it applies:

(i) where you are **offering goods and services** to people in the EU (whether for money or not); or

(ii) where you are **monitoring the behaviour** of people in the EU (where that behaviour takes place in the EU).

In this case, in most circumstances you will need to appoint a representative in the EU.

(c) In many cases this will be obvious. For example, a London office of a UK company decides to employ staff or build up a database of supporters as part of a campaign that it is running. In other cases it can be less clear and you may wish to consider taking legal advice.

(d) It should be noted that GDPR includes a regime for the ICO and its counterparts in the rest of the European Union to collaborate, in the case of processing which takes place in multiple EU countries (or "substantially affects" multiple EU countries). In this case, a "lead supervisory authority" will take the lead, and consult with other relevant supervisory authorities. This Guide assumes that the relevant supervisory authority is the ICO.

Transparency

5. A cornerstone of the European data protection regime is that, so far as practicable, individuals should have a right to understand who is processing their data and why, and to receive such other information as is necessary to make the processing "fair".

6. This obligation has typically been addressed by organisations with a 'privacy notice', which have often historically been written in fairly vague terms and have resembled "terms and conditions" which in practice, few individuals would read. GDPR has consequently introduced more detailed requirements about what people need to be told, and how they need to be told it.

7. This obligation to provide information does not always sit naturally with the activities of campaigning and advocacy bodies, which (as stated above) may wish to process large amounts of personal data to persuade people of their cause, and also may wish to consider where to target often limited resources.

It may be seen as disproportionate, for example, to post each individual a letter explaining what is happening with their data. However, in most cases, the obligation applies whether or not the individuals have received the personal data directly from the person, and organisations need to consider how they should structure their activities so that they can provide the required information.

What do we need to say?

8. There is now a list, set out in GDPR. The ICO also summarises the requirements in guidance. The required information includes, in broad terms:

8.1 **Who you are.** The identity and contact details of the controller, its EU representative (if any), and the contact details of the data protection officer (if any);

8.2 **What you are doing with their details.** Why you are processing the data, and your legal basis for doing this (discussed below). Where you are justifying the processing as being in furtherance of your "legitimate interests" (or someone else's), you also need to say what those interests are, and when you are using "consent", you need to tell people that they can withdraw that consent at any time.

8.3 **Who you are going to share the details with**. This includes controllers and processors. You need to either name the recipients, or identify them by clear categories;

8.4 **The fact that you plan to transfer the data outside of Europe**. Also, whether the European Commission has decided that the third country has an adequate level of compliance and what steps you are taking to ensure compliance;

8.5 **How long you will keep their details** or the criteria that you will use to determine this;

8.6 **What their rights are.** These need to be spelt out – including the right to access their data, to rectify it if inaccurate, to have it erased or restrict its use, to object to processing, and the right to data portability. You should set these rights out and explain that they do not apply in all circumstances. You also need to tell people that they can complain to the supervisory authority (as stated above, in the UK, this is the ICO);

8.7 **Whether they have to provide you with the information to comply with statute law or a contract (or to enter into a contract)**, and what happens if they don't. This is only needed where you are getting the information directly from the person.

8.8 **Where you got the personal details from.** You only need to tell individuals where you have not obtained the data from the person directly. In these circumstances, you should also state whether it came from publicly accessible sources.

8.9 **The categories of personal data that you are processing**. This only applies if you have not obtained the data from the person themselves.

8.10 **Whether you engage in automated decision-making, including profiling, if this produces legal effects or similarly significantly affects the person.** If this applies you also need to tell people the logic involved, and what this means for the person. The ICO has stated that this

may apply in the case of certain more sophisticated actions where campaigns or political parties use data analytics to identify the specific interests of individuals and tailor their messaging to that individual accordingly (known as "micro-targeting")[1]; and that the impact of this could be assessed in a data protection impact assessment (see paragraph 20).

8.11 If you intend to further process the data for different purposes, before doing so you need to provide the individuals with further information as appropriate.

How should we say it?

8.12 GDPR has an emphasis on ensuring that privacy notices are concise, transparent, intelligible and easily accessible; and written in clear and plain language (particularly where addressed to a child).

8.13 You should look to provide the information in "layers". Using this approach, the individual is provided upfront with an overview of who you are, and what is happening with their data. There are no absolute criteria about what should be included in this top layer – but as a general rule, you should look to include information that may be surprising to a person or that otherwise may not be in their reasonable expectations. Without attempting to be exhaustive, this could include a summary of data sharing and profiling activity, for example. You could also set out, in summary, the individual's rights, including their right to object (which, GDPR says, must be "*explicitly brought to the [individual's] attention…and…presented clearly and separately from any other information*"). This top layer should then be linked to more detailed information – commonly set out in a "privacy notice", which describes your data processing.

8.14 For example, A Ltd is holding a campaign to increase the minimum wage. On its website, it asks people to enter their name and email address to register their attendance. It plans to send this list and content to a processor, who will email the individuals with information with the start time and place of the event. Above the "submit" button, A Ltd tells people that their details will be processed by A Ltd for the purposes of emailing them about the event, and that it will be shared with a processor for this purpose. It also tells people that it will use their information to forecast attendance at the event. It tells them that they have rights over their data, including the right to object to processing in some circumstances. The individual is then referred (with a hyperlink) to a more detailed privacy notice, containing more detail and the remaining information above.

8.15 However, there will often be more complex circumstances: for example, where you have obtained the personal data from another source (which collected it) – such as an online petition platform; or where you have obtained it yourself, but indirectly. In the latter category, in previous guidance the ICO gave examples of 'inferred' data, where algorithms are used to analyse data to profile people – e.g. credit scoring; 'observed' data – e.g. by tracking people online; and 'derived' data, by combining other data sets. Such methods of data processing are as relevant to some organisations engaging in campaigning activity, and seeking to target a message effectively, as to commercial organisations looking to sell products. You should think about how to provide the information in these circumstances. Please note the other requirements and regulatory

1. See also the ICO "Democracy Disrupted" guidance referred to at the end of this Guide.

guidance which may apply (and also should consider what action your organisation should take to ensure that the data has been lawfully collected and is appropriate to use) – for example, restrictions on sharing data for direct marketing purposes in the Fundraising Regulator's Code of Fundraising Practice.

8.16 In its guidance, the ICO emphasised that it welcomed innovative approaches to providing privacy notices, giving the examples of "just-in-time [pop-ups which provide limited privacy information when the individual clicks on the relevant field – for example, to populate their email address]; video; the functionality of devices and privacy dashboards", and that "[a] blended approach, incorporating a variety of these techniques is likely to be the most effective". Organisations might also use symbols and icons, and it may be that sectors (such as the charity sector) or activities (such as emails promoting a campaign) come to adopt set icons that are understood to mean particular things.

8.17 There are some exceptions from the need to provide a privacy notice in particular cases, including where the individual already has the information and (where the data is indirectly collected) where providing the information is impossible or involves disproportionate effort (this has historically been narrowly construed – GDPR states that it applies "in particular" for archiving in the public interest, scientific and historical research purposes and statistical purposes) and insofar as complying "is likely to render impossible or seriously impair the achievement of the objectives of [the] processing"; where European Union or member state (e.g. UK) law has expressly authorised the disclosure; or where there is an obligation of professional secrecy. The DPA contains further exemptions to the requirement to provide the information in some cases: for example, it is not necessary to provide the information insofar as doing so would be likely to prejudice the prevention and detection of crime. However, these exemptions are generally narrowly construed and you should look to take legal advice when relying on one. However, as stated below, in many cases – such as sending promotional emails - you will likely need the individual's consent in any event.

8.18 As an action point, if you have not already done so, it is advisable to map out what data processing you undertake, and consider (potentially with legal advice) the amendments that need to be made to your privacy notice (in different layers) to comply with the requirements.

Not "Direct marketing" and consent

9. As stated above, completely separate from GDPR, PECR regulates e-marketing activity.

10. In a campaigning context, 'direct marketing' is something of a misnomer. Relying on a tribunal decision (about automated telephone calls made to voters by the Scottish National Party), the ICO takes the view that any message "*promoting an organisation's aims and ideals*", including "*the promotional, campaigning and fundraising activities of not-for-profit organisations*" is covered.

11. Taking this as a starting point, under the current law, your organisation:

    (a) Requires an individual's consent to send campaigning messages to individuals by electronic means, including email and SMS, or to make automated calls;

(b) Is required to screen a number against the Telephone Preference Service[2] before using it for a live telephone call for campaigning purposes (and if the number is registered with TPS, only phone the number with consent); and

(c) Under *GDPR*, must maintain a suppression list of individuals who have opted out of direct marketing communications by any form (including post). Charities should also be aware of the Fundraising Preference Service, which is an avenue by which individuals can exercise this right. The FPS generally sends suppression requests for individuals to the email address listed on the Charity Commission's website – however, individuals can also contact organisations (whether charitable or non-charitable) directly.

12. Consent is currently defined in this context as a "*freely given, specific and informed indication of… wishes*", and consent also needs to be "*unambiguous*" and "*by statement or clear affirmative action*", and there are specific requirements about how it should be structured, and the level of detail which is provided. The ICO has detailed guidance on approaches to obtaining valid consent. Consent should be clear and specific and not bundled together with other services – for example, you should not seek to obtain consent by asking someone to tick to say they have read and agree to a privacy notice, which states (as part of a long message) that you will send campaigning emails.

13. Organisations should keep the position under review over the coming months (taking legal advice where necessary), as the new law, the ePR takes shape.

Legal bases for processing

14. Returning to the GDPR: wherever these rules apply, unless you have identified an exemption (discussed briefly above), it is necessary to find a legal justification for any data processing – known as a legal basis (or more formally, a "condition for processing").

15. As we mention above, under GDPR, controllers need to specify, in their privacy notice, which legal bases they are relying on, meaning that it is particularly important to attempt to identify one (or more) in respect of any current activities, and as part of the process of formulating new activities.

16. There are six main conditions to choose from, which can be briefly summarised as follows:

(a) The individual has **consented** to the processing;

(b) The processing is necessary for the **performance of a contract** with the individual (or to take steps at the individual's request before entering into the contract);

(c) The processing is necessary to comply with a **legal obligation**, except a contract;

(d) The processing is in the **vital interests** of the individual or someone else (generally life and death situations);

(e) The processing is necessary in **furtherance of various public functions**/for the administration of justice etc.; or

2. There is also a regime called "soft opt-in". This is a limited right for an organisation to send promotional electronic messages (by e.g. email and SMS) without explicit consent, to advertise goods and services to people who have recently brought similar goods and services. The ICO's view is that it is not applicable to charity fundraising and political campaigning activities, but it may be relevant to other aspects of your activities (for example, if your organisation runs an online shop).

(f) The processing is necessary for the **legitimate interests** of the controller (or someone else), except where this is unwarranted because it prejudices the rights and freedoms/legitimate interests of the individuals.

17. When carrying out campaigning activity, your organisation may particularly frequently consider (f) (**legitimate interests**), or (a) (**consent**).

(a) In short, legitimate interests requires a 'balancing act' to identify whether:

(i) the processing is necessary for the purposes of the controller, or another organisation;

(ii) it is, in any event, "overridden" by the interests or rights of the individuals.

(b) Under GDPR, specific consideration should be given where the individuals are children. As part of the analysis, you should also consider whether individuals would reasonably expect you to have processed the data in a particular way. A common way to conduct the balancing test is to carry out a so-called "legitimate interests assessment", a topic on which the ICO has released guidance. Please note that legitimate interests cannot be used by public authorities in many circumstances.

(c) As an alternative, consent can be used. As stated above, the definition of consent is stricter under GDPR than was previously the case. Additionally, clear evidence of consent will need to be retained, and there are separate rules about obtaining parental consent in relation to processing of children's data, and so on. As mentioned earlier, where the processing is electronic or automated telephone "direct marketing", or marketing calls to TPS-registered numbers, under the current law you will need consent (or, for live phone calls, for an individual to indicate that they do not, for the time being, object to being called) anyway[3], meaning consent may be the appropriate basis for processing. You should note that GDPR states that "it shall be as easy to withdraw as to give consent", and so (as is currently the case) wherever you plan to rely on consent, you should consider how they will facilitate and process subsequent 'opt-outs'.

18. In addition, where you are processing:

(a) **Special categories of data** (that is, information about a person's political opinions, race or ethnicity, religious or philosophical beliefs, trade union membership, sexual orientation, sex life, health, genetic data or biometric data (insofar as you are using it to identify someone) you need to identify an *additional* legal basis. These are set out in Article 9 of GDPR, and in the DPA: there are a large number of them and you may wish to seek advice on which can be relevant. **Explicit consent** of the individual is a relevant basis, while it may not always be feasible. Another is where processing is carried out by a **not-for profit body** with a political philosophical, religious or trade union aim where that processing relates solely to the members or former members of that body, or to people it contacts regularly in connection with its purposes (but note that this condition cannot be relied upon to disclose data outside of that body). A third is where the processing is **manifestly made public** by the individual themselves. There is also a condition for processing data relating to political opinions, by

3. See footnote 1 on "soft opt-in"

bodies registered under section 23 of the Political Parties, Elections and Referendums Act 2000. Often, various conditions need to be met for a legal basis to apply, so it is important to consider this carefully and seek advice where appropriate.

(b) **Data on criminal convictions and offences** and related security measures – you will also need to identify a legal basis set out in Article 10 of GDPR and the DPA.

Other principles

19. The above are some of the most pertinent considerations which your organisation will need to consider when it wishes to engage in campaigning activity. However, to an extent it is the 'tip of the iceberg' and there are a number of other important requirements in the GDPR that you must consider. As key examples, there are requirements:

    (a) That personal data must be processed lawfully, fairly and in a transparent way. This is partly dealt with by the provision of privacy notices, but you should also note that the processing should also generally be fair (and so, the ICO notes, unduly detrimental, unexpected or misleading) and not breach other legal requirements (such as a duty of confidence to the person).

    (b) That personal data is collected for specified, explicit and legitimate purposes (this should be clear in the privacy notice) *and not further used in a way which is incompatible with those purposes* (known in GDPR as **purpose limitation**). If you use it for purposes which are different but not "incompatible", you will generally need to provide a further privacy notice.

    (c) That personal data should be accurate and, where necessary, kept up-to-date (**accuracy**);

    (d) That personal data should be adequate, relevant and not excessive (**data minimisation**). So you should not be collecting personal data which you do not need.

    (e) That personal data should not be kept for longer than is necessary for the purposes for which it is being processed (with some exceptions – for example, for scientific or historical research purposes in some cases) (**storage limitation**); and

    (f) That there should be appropriate technical and organisational security measures in place, including protection against unauthorised or illegal processing, loss, destruction and damage (**integrity and confidentiality**).

20. GDPR introduces a new requirement – that a controller must be able to show that it has complied with the rules above (**accountability**). This has always been good practice (and sensible in the case of any regulatory scrutiny), but is now obligatory. A key (but non-exhaustive) way to demonstrate this is to have proper policies in place, demonstrating that you have considered the above rules; to implement these policies in practice and to demonstrate how they are being complied with. You can also demonstrate this by having proper contracts in place with processors, and proper security measure in place. Additionally:

    (a) GDPR requires most organisations (controller or processor) to keep a record of their processing activities. The ICO provides guidance on how to do this, and a template spreadsheet (the guidance is referred to below).

(b) GDPR also contains a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities – rather than addressing data protection compliance as an afterthought. In relation to any significant new activities it is therefore good practice at the outset to conduct a data protection impact assessment (**DPIA**) to assist in identifying and minimising the data protection risks of a project. It is now obligatory to conduct a DPIA if you consider that it is likely to result in a high risk to individuals (and in some cases, having conducted one, to consult with the ICO about the processing)

Other issues

21. *Individuals' rights*

GDPR increases the rights of individuals over their personal data. In particular, they have rights:

(a) To access a copy of their personal data, and receive certain information about how and why it is being processed – in broad terms, this is the same as the concept of a **subject access request** which existed under the old law. As a general rule, subject access requests must now be dealt with within one month, and dealt with free of charge – while there are limited circumstances in which this can be expanded (to up to three months) and/or a charge can be made.

(b) To **object** to the use of data where the controller is relying on the "legitimate interests" or "public task" bases, or using the data for direct marketing (discussed above) or certain research / statistical purposes. GDPR requires that this right must be brought prominently to the individual's attention, at the latest, when you first communicate with the individual.

(c) In some cases, to ask you to **delete** their personal data from your records;

(d) To **correct** inaccurate records;

(e) To **restrict** your use of it, generally if there is a disagreement about accuracy or legitimate use.

(f) For the information to be provided in a format which can be 'ported' over to another service provider ("**portability**").

(g) Rights in respect of **"automated decision-making"**.

These rights do not apply in all cases. However, any request received should be treated seriously (given potential penalties for non-compliance) and generally all staff in the organisation should be trained to recognise such a request and forward it to an appropriate person at your organisation, who can deal with it (with external legal advice as appropriate). In many cases it is also necessary to collaborate with organisations with whom you have shared the data – for example, if asked to rectify someone's details, you generally will need to tell everyone with whom you have shared the old, incorrect details.

22. Exporting data

As under the law in place before GDPR, there are rules that data must not be transferred to a country or territory outside of Europe unless there are adequate levels of protection for the rights and freedoms

of individuals in relation to their data. Some countries have been deemed by the European Union to have an "adequate" level of data protection compliance, but otherwise it is necessary to take other specified steps – such as putting in place a prescribed contract (known as **model contract clauses**) with the overseas recipient of the data – to ensure compliance. If and when the UK leaves the European Union, bodies exporting data from the EU to the UK will also be subject to these restrictions - unless and until the European Union finds that the UK has an "adequate" level of compliance.

23. Data Protection Officers

Some organisations will be required under GDPR to appoint a Data Protection Officer (**DPO**), including public authorities, but also organisations whose **core activities** consist of **regular and systematic monitoring of individuals**, or **processing sensitive data** on a **large scale**. While there are no specific qualification requirements, a DPO must be designated "*on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices*". There are also rules about how the DPO is treated – for example, they may not be dismissed or penalised for performing their tasks (similar to protection from sanction that is given to whistleblowers); they must report directly to the highest management level of the organisation; and other jobs given to them as part of their role must not conflict with their role as a DPO (which, it is thought, removes most senior managers at an organisation and certain others from being able to be the DPO).

24. Automated decision-making and profiling

GDPR specifically regulates the act of making decisions by solely automated means (including profiling) where those decisions have legal or "similarly significant" effects on a person. These terms are not defined, but the ICO gives examples of (i) refusing a credit application; and (ii) turning someone down for a job. The specific restrictions only applies where there is no human involvement in the decision-making process). This activity is only allowed in specific circumstances.

25. Breaches

Unlike the previous law, GDPR is prescriptive about what controllers and processors must do if there is a security breach (leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data). In short:

(a) It is now obligatory for a controller to report breaches to the ICO, generally within 72 hours of becoming aware of them, if it is likely that it will impact upon people's rights and freedoms. There is a requirement to provide particular information when reporting the breach – but if you don't have it all within 72 hours, it is permissible to provide the information as soon as possible in phases.

(b) Breaches must be recorded, whether reported to the ICO or not.

(c) Where a controller determines that a breach is likely to result in a high risk to individuals, it is necessary to tell those individuals without delay (again, there is prescribed information which you need to include).

(d) Processors are required to tell controllers without undue delay as soon as they become aware of a breach. This must be a requirement in the contract between the controller and

the processor. This allows the controller to comply with the requirements above (e.g. to notify the ICO).

26. Cookies etc.

Separately, if your organisation uses "cookies" or similar technology, you have obligations to be transparent with people that you are using them and why, and obtain a person's consent to store the information on their device (except when the cookies / trackers are "strictly necessary" - rather than just helpful or convenient - to provide the service being requested by the person). Organisations may wish to seek legal advice on cookie policies and means of obtaining consent.

27. Data protection fee

The previous requirement to "notify" the ICO that you are a controller has been replaced by a requirement to pay a fee to the ICO and, as part of this, provide various pieces of information. The level of fee largely depends on the size of organisation, while there are some exceptions (for example, charities pay the lowest level of fee). There is a link to ICO guidance about this at the end of the guide.

28. Data sharing

The ICO is also in the process of updating its data sharing code of practice. When published, the principles in the revised code should be considered closely.

Penalties

29. Organisations will already be aware of the vastly increased potential fine (now up to 4% of global turnover or €20 million) for the most serious breaches of GDPR. At the time of writing, the highest fines actually implemented by the ICO are at £500,000 (in one case for a data breach, in another for alleged breaches of transparency and security rules), which was the maximum fine under the previous law. However, the ICO has also announced (on 8 July 2019) its intention to fine British Airways £183.39 million for a data breach which occurred since GDPR came into force.

30. The ICO also has powers under GDPR and the DPA including:

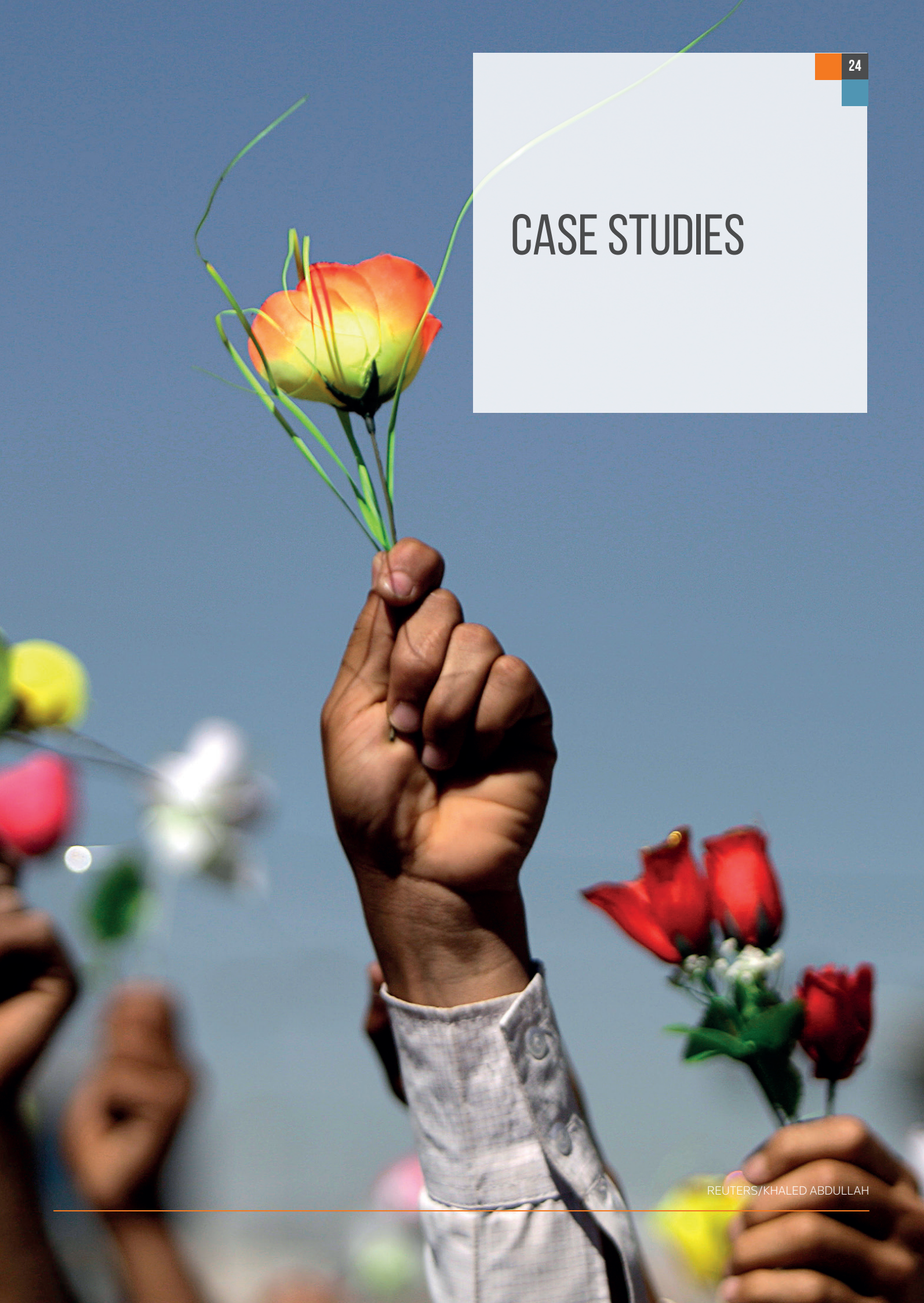
    (a) To require controllers and processors to provide it with information (through an **information notice**);

    (b) To audit a controller or a processor (through an **assessment notice**); and

    (c) To direct a person to take (or not to take) particular steps (an **enforcement notice**).

31. Organisations should take the potential for significant penalties into account when contemplating the risks of data protection non-compliance.

CASE STUDIES



REUTERS/KHALED ABDULLAH

CASE STUDIES

A non-profit organisation that campaigns to reduce homelessness sends emails or letters to their existing supporters to raise awareness about the solutions to the problem. Sometimes they cold-call people to talk about the issues and to ask for a financial donation. Recently, they started getting complaints that they were sending too many emails and people were getting annoyed when they were called. They would like to know if they are breaking any laws and to understand the steps they should take to ensure that they meet privacy and data protection requirements.

The charity should go through the points raised above. It might address the issues as follows:

1. **Is the non-profit processing personal data?**

   Yes, it plans to use names, postal addresses and email addresses, as a minimum. This is personally identifiable information about living individuals, and so GDPR applies.

2. **Is the non-profit a controller or a processor?**

   (a) It is presumably determining why people are being contacted (to be asked to donate), and how, so it is a controller and is responsible for the bulk of compliance with GDPR. If it does not do so, it may face regulatory action including fines of up to €20 million or (if higher) 4% of global turnover.

   (b) It should consider whether it is using another person/company (other than its employees) to process information on its behalf – for example, perhaps it sent the information to another company to type up into a spreadsheet or upload to a software system. If it does, it should consider whether it has an appropriate data processing agreement in place with that other organisation, and whether that complies with the strict specifications in GDPR.

3. **Data protection by design and by default.**

   As part of deciding to embark on the activity, it should consider the data protection implications of doing so. In this case, is it likely to annoy or upset people? Is it likely to be invasive? What steps can it take to minimise this (for example, only calling at fixed times of day, putting a limit on the number of phone calls and respecting opt-outs?). It may consider doing a data protection impact assessment.

4. **Now it knows that the data protection regime applies to the activity, has it provided appropriate privacy notices to people?**

   (a) The existing supporters may have been recruited directly, and as such should (under GDPR) have been provided with privacy notices at that point. These privacy notices should have included all of the prescribed information – perhaps

a short notice with key information, linking to a more detailed privacy notice. The non-profit should particularly check that it has not said that it will not embark on this kind of activity. It may be breaching the first, but also the second data protection principle if the proposed emails are incompatible with the purposes for which the data was collected.

(b) If the supporter details have come from a third party, it should (under GDPR) also have provided privacy notices to people within the time limits set out in GDPR.

(c) If it is proposing to mix some of its own information (e.g. names and addresses) with other information (e.g. telephone numbers sourced externally), there are a number of issues to be aware of, and it should exercise caution. A basis of the recent fines levied against a number of charities was that such "data matching" was not made sufficiently clear to individuals and was unfair.

5. **Separately from the data protection requirements, has it contained the necessary consents to comply with e-privacy laws?**

(a) Activity to promote the non-profit's activities (relieving homelessness) and to ask for a donation is likely to fall within the ICO's definition of "direct marketing". This means that:

- The non-profit should have obtained prior consent to send emails to individuals;
- Under the current law, it should have screened against TPS before engaging in the telephone calls;
- It may wish to check the names against the Mailing Preference Service list (this is a condition under the Code of Practice of the Direct Marketing Association, which is relevant if the non-profit is a member);
- It should be keeping suppression lists, allowing people to opt-out of direct marketing by any channel.

(b) Was the consent compliant? For example, was it *specific, informed, freely given, unambiguous, and given by statement or clear affirmative action?* Is it sufficiently granular? Has it been properly documented? The ICO has issued detailed guidance on consent and GDPR.

6. **What legal basis (/ bases) does it have to process data?**

(a) Subject to the considerations above, the non-profit may have initially had valid consent to direct marketing. There is no specific evidence that it is processing special categories of personal data (for example, information about a person's health), but if it was, that could also be justified by 'explicit consent', as long as the strict definition of this was met.

(b) Alternatively (and assuming that it is not using special categories of personal data) it may have determined that contacting people is necessary to further its legitimate interests, and (having conducted a balancing act) that it is not overly intrusive.

(c) However, it appears in this way that the non-profit is acting in a way which is causing complaints, which may cause it to reconsider whether it properly satisfies the condition. What will help this analysis will be the consideration, suggested above, of the potential impact of the processing on individuals, and mitigating steps.

7. **What are the other key considerations?**

The non-profit should consider whether it is complying with the other data privacy requirements detailed above. For example, is it holding onto personal data disproportionately? Is it exporting it outside of Europe to process it, without appropriate arrangements in place? It should adopt or review its internal data protection policies, and take steps to demonstrate how it is complying with the relevant requirements.

It should also consider whether other industry- or activity- specific rules and guidance apply to it (which are not explictly addressed in this Report) such as the Fundraising Regulator's Code of Fundraising Practice, or Charity Commission and / or Electoral Commission guidance.

TIPS AND FURTHER READING

REUTERS/ANINDITO MUKHERJEE

TIPS AND FURTHER READING

- Map out when your organisation is using personal data, when you are a processor and when you are a controller, and (where you are a controller) what legal basis (/bases) you have to undertake the activity.
- As a controller:
  - » Review privacy notices. Consider whether there are circumstances in which you may not be complying with transparency rules and whether you need additional advice.
  - » Where you rely on consent for any reason – whether to process a supporter (or potential contact)'s details or to send campaigning emails, check that it meets the high threshold set out under the GDPR and is properly documented. Put in place mechanisms to record when consent is withdrawn.
  - » Put agreements in place with processors, with the prescribed information.
  - » Introduce policies and train staff on the obligations in GDPR, and the rights that individuals have. For example, could any member of staff who received one recognise, and know how to deal with, a "subject access request"?
  - » Be aware of the data protection fee and pay it as appropriate.
  - » Consider how to comply with GDPR more generally – for example, if exporting data outside of Europe, how is this justified?
- As a controller or a processor:
  - » Have a policy for what to do in the event of a data breach.
  - » Keep a record of processing where required.
  - » Consider whether or not you are required to have a DPO.

» Put appropriate security measures in place.

Links / further reading

1. Information Commissioner's Office:
    - » *Guide to the General Data Protection Regulation (GDPR)* - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
    - » *Guidance on Political Campaigning* - https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf
    - » *Democracy Disrupted? Personal information and political influence* - https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf
    - » *Right to be informed* - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/
    - » *The data protection fee: A guide for controllers* - https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf
2. Article 29 Working Party (a European-level advisory body made up of representatives from data protection authorities; on 25 May 2018 it was replaced by the European Data Protection Board (**EDPB**)) on transparency - http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
3. European Commission: *2018 reform of EU data protection rules* https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
4. Fundraising Regulator, *Code of Fundraising Practice* https://www.fundraisingregulator.org.uk/code-of-fundraising-practice/code-of-fundraising-practice/
5. Bates Wells GetLegal data protection policy (to be tailored as appropriate in light of your organisation's specific campaigning activities) - https://getlegal.bwbllp.com/

THOMSON REUTERS
FOUNDATION

www.trust.org