The Information Commissioner's response to the Public Administration and Constitutional Affairs Committee's inquiry into fundraising in the charitable sector

1. The Information Commissioner has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations (EIR) and the Privacy and Electronic Communications Regulations. The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

Introduction

2. The Information Commissioner welcomes the opportunity to respond to the inquiry into charity fundraising because recent allegations raise questions about the sector's compliance with data protection law and the rules on electronic marketing, particularly in relation to making cold calls to people registered with the Telephone Preference Service (TPS) who have not given their prior consent. There has also been considerable comment about apparent weaknesses in the self-regulatory system and that poor practices appear to have been allowed to develop relatively unchecked. Not all of the alleged practices are related to data protection but the initial findings of our investigation show that there are significant risks of non-compliance with the direct marketing rules and related areas of practice, such as records management.

What the law says

3. Under the Privacy and Electronic Communications Regulations a charity contacting individuals to appeal for funds or support for a campaign must comply with direct marketing rules and data protection law. That means checking whether someone is on the Telephone Preference Service (TPS) list before calling them. Where someone is listed on the TPS, charities and fundraisers may only call where they have specific permission from the subscriber to do so. Charities must also comply with the requirements of Data Protection Act, including the eight data protection principles, when collecting, using personal data or obtaining data from third parties. A detailed explanation of the law can be found in the annex below.

Specific questions

Extent of poor fundraising practices and impact on members of the public

4. The ICO has received relatively few complaints from the public about receiving nuisance calls from the charity sector, even following extensive coverage in the media. In the absence of significant volumes of complaints about fundraising, our engagement work with charities has focused primarily on addressing concerns about the records management and IT security of small and medium charitable organisations through a series of advisory visits and workshops. We have considerable evidence of complaints about direct marketing in the private sector and this is where our enforcement activity has been previously focused. We have been investigating unlawful practices by fundraisers which appear to target vulnerable people.

5. We are investigating a number of charities and call centres following allegations made in the Daily Mail. We have made contact with each of the organisations named in the Daily Mail and we have requested information about their compliance with the Data Protection Act (DPA) and the Privacy and Electronic Communication Regulations (PECR). We are in the process of meeting representatives of the charities and third party fundraising organisations. Our evidence at this stage will focus on the initial findings of our current investigation into fundraisers' compliance with data protection law and electronic marketing rules and the impact on members of the public. Wider questions about the extent of the problem, the number of people affected and the percentage of money raised by private contractors are best addressed by the self-regulatory fundraising bodies and the Charity Commission.

6. During the course of our current investigation into allegations made by the Daily Mail it has become apparent that organisations such as the FRSB and the TPS have received complaints from members of the public in significant volumes. As part of our investigation, we have received information on complaint volumes from the FRSB. These volumes are substantially more than those received by the ICO. Although we do not have specific details of each individual complaint, we have received a full break down of the charities against live calls, sms, emails. The FRSB provided us with totals of complaints as follows: SMS: 421; telephone: 8056; and email: 2522. The total is 10,999 across 220 organisations. We do not yet have detail of what these complaints are about in terms of tone of marketing and method etc. We shall use the information from the FRSB to support our investigations and potential enforcement action and compliance strategy. As part of our wider education and awareness work in this sector we shall also be writing to a further 80 plus charities over the coming months. According to a PwC report in 2014, the public made

48,432 fundraising complaints to FRSB member charities in 2013. We are in the early stages of developing an MoU with the FRSB to share intelligence data.

Initial findings

7. Our initial findings indicate that many charity fundraisers operate along similar lines to any other marketing business, especially in areas such as lead generation, telephone marketing techniques, buying in of contact lists and in the way they outsource. There are some differences, for example the practice of list swapping or sharing amongst fundraisers, which can lead to individual donors being targeted and called by numerous charities. We also have concerns about the collection of information on the street or the door-step. We are looking at how personal data collected by chuggers finds its way from this street transaction into subsequent unsolicited calls from the charities represented as well as "affiliated" charities.

8. It is evident from our meetings with charities that they do not have accurate and reliable records on whether donors have consented to marketing. Work to test the organisations' due diligence and identify when and where individuals' consent was obtained has only happened as a result of our investigations. There are also weaknesses on the wording of privacy policies, retention policies and opt-in/out wording. Some retention periods of data are for extremely long periods.

9. From the responses received to date, all the charities appear to recognise they need consent in order to make marketing calls to individuals registered on the TPS. However, there seems to be little understanding that the calls made to TPS customers to gather consent for the specified charities to contact them require prior consent.

10. The charities appear to be employing third party call centres and allowing them to obtain data leads, without properly understanding that very often the charity is responsible for any non-compliance issues by the third-party.

11. Some charities are assuming consent at the time of donation. For example, some fundraisers are assuming that by submitting details to sign up to a direct debit, an individual is agreeing to be contacted by phone, text or email.

12. In many cases opt-outs are only available by emailing, writing or telephoning on behalf of the member of the public making the donation, rather than having an opt out at the point of data collection. Our guidance is that organisations should adopt opt in as best practice.

13. There is confusion about the law, not helped by the sector's concept of "warm donors" which is covered in the Institute of Fundraising's code of practice and the reluctance shown by the IoF and some of its members to accept that charities have to follow the same direct marketing rules as any other organisation.

14. Our written guidance has always made it clear that calling a subscriber registered on the TPS, or who subsequently registers on the TPS, without their prior consent would breach PECR.

15. Prior to issuing our Direct Marketing guidance in 2013, however, our approach to taking enforcement action was a pragmatic one. Our earlier guidance (2005–2013) said we would not enforce against charities contacting regular supporters on the TPS unless we received complaints. This position was based on a level of trust with the sector at that time and the sector has evolved significantly in its use of marketing techniques over the last ten years. We did urge a cautious approach at the time and trusted that charities would follow this advice responsibly. Some fundraisers appear to have interpreted this as an exemption from the law and this view does not appear to have been challenged by the self-regulatory bodies. It is difficult to see how some of the current methods of gathering sign-ups to direct debits, high pressure telephone techniques or buying in or swapping of lists equates to the sort of long-established relationship envisaged in our earlier guidance.

16. Our direct marketing guidance published in September 2013[1] removed the reference to the ICO only taking action where we received complaints. When we began our investigation into charities it became apparent that there was a need to improve fundraisers' understanding of PECR rules. This lack of understanding has not been helped by the fact that until 18 August the IoF code continued to refer to the regulatory approach set out in an old ICO good practice note which was withdrawn in 2013. This highlights our concerns about the absence of due diligence.

Government's proposed legislative changes and any further action

17. The first principle of the Data Protection Act is to process people's information fairly and lawfully. A good start in re-building public trust and confidence would be for the fundraising sector to demonstrate a commitment to comply fully with the data protection laws that already exist. Instead of lobbying for concessions, we would like to see charities and their self-regulatory bodies take responsibility for making sure that fundraisers comply with the law and respect the choices of individuals who have registered with the TPS and have not given specific permission for charities to call them.

[1] https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

18. Self-regulation can work effectively but sector bodies have to keep up with changes in the law and the regulatory priorities of statutory regulators otherwise they risk causing confusion. At the very least compliance with the law should be the minimum standard expected of their members. Our statutory guidance about the issue of monetary penalties states that in considering both whether to impose a penalty and the amount of any penalty we will have regard both to adherence to relevant codes of practice or guidance published by the Commissioner or others and to the extent to which the data controller has already complied with any requirement or rulings of another regulatory body[2].

19. Charities need to understand that usually they are data controllers for fundraising carried out on their behalf and have overall responsibility for compliance with the law. They should identify potential privacy risks in fundraising activities and make sure they set up policies, procedures and provide training to ensure employees, volunteers and third parties fully understand their responsibilities. There is initial evidence that some charities have included strict requirements in contracts but may not have monitored them effectively. It is very likely that the charities themselves have received complaints and these should have rung alarm bells.

20. There are a number of enforcement tools available to the Information Commissioner's Office for taking action against anyone who breaches the Privacy and Electronic Communications Regulations (PECR). They include criminal prosecution, non-criminal enforcement and consensual audits. The Information Commissioner also has the power to serve a monetary penalty notice imposing a fine of up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010 or serious breaches of the Privacy and Electronic Communications Regulations occurring after 26 May 2011.

21. On 6 April 2015 the threshold for issuing monetary penalties under PECR changed. An amendment to the Regulations removed the requirement for the ICO to be satisfied that the contravention is of a kind likely to have caused substantial damage or substantial distress. The ICO will be able to issue a penalty for any serious contravention of regulations 19 to 24 in PECR (these provisions cover automated calling and direct marketing). We have consulted with the Secretary of State on a revised version of the monetary penalties guidance issued under section 55C (1) of the Data Protection Act 1998, which will shortly be laid before Parliament.

22. On some occasions it is not the "data controller" itself that is responsible for data protection breaches – it is an individual who is working for or contracted to the data controller, acting in contravention of the

[2] https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf

organisation's policies and procedures, or an individual who obtains information from the organisation without their knowledge or consent. Section 55 of the DPA makes it a criminal offence to knowingly or recklessly and without the consent of the data controller obtain, disclose or procure the disclosure of personal data. This offence is currently punishable by fine only.

23. The Criminal Justice and Immigration Act 2008 includes a provision for introducing custodial sentences for the DPA section 55 offence in section 77, but this has not been commenced. The Information Commissioner continues to call for more effective deterrent sentences, including the threat of prison in the most serious cases, to be available to the courts to stop the unlawful use of personal information. Lord Justice Leveson recommended that the necessary steps should be taken to bring the provisions into force. Since the publication of his report, the Parliamentary Joint Committee on the Draft Communications Data Bill has added its voice to those of the House of Commons Justice and Home Affairs Committees in calling for sections 77 and 78 of the Criminal Justice and Immigration Act 2008 to be brought into effect.

24. The deliberate misuse of a vulnerable person's information could justify the possibility of a custodial sentence for the most serious offences. With the removal of the fine only regime, the Courts will also be able to impose punishments that more effectively fit the crime. The possibility of a custodial sentence opens up a range of lesser penalties that are not currently available. Community service orders, curfews and tagging may be more effective in their deterrent power than small fines mitigated by an offender's modest ability to pay.

25. For example, a manager of a car rental company was prosecuted by the ICO for a section 55 offence in July 2014. He stole the records of almost two thousand customers, who had recently been involved in a road traffic accident. He sold them to a claims management company, in order to use the data as leads to sell on to solicitors to make personal injury claims. He pleaded guilty at the first opportunity and was fined £500, ordered to pay costs of £264.08 and a £50 victim surcharge.

26. We have seen incidents where data is obtained from consumers and then sold commercially and later re-sold. The trends are concerning as we are now seeing personal data collected legitimately being obtained unlawfully by criminals who then sell the data to commercial companies within the claims management industry. The ICO are currently conducting a number of other criminal investigations involving Claims Management Companies (CMCs) who we believe are responsible for unlawfully obtaining personal data. There is a risk that data sold and shared by fundraisers could be similarly targeted.

Charities' values and interaction with the public

27. Our experience in other sectors shows that overall responsibility for ensuring compliance with data protection needs to be taken at board level in order to demonstrate a commitment to comply with the law and to drive up standards. Larger charities with effective information governance have sought to appoint or designate data protection officers with the ability to report at board level. Charities should not treat fundraising as a separate activity only covered by marketing rules. They must also consider their wider data protection obligations to treat people fairly and in line with their expectations.

28. When charities are considering aggressive marketing campaigns or novel ways of fundraising we recommend they undertake a privacy impact assessment (PIA) alongside any ethical considerations, to make sure privacy risks are properly understood and safeguards put in place. The ICO has published a code of practice on privacy impact assessments[3] that could be used as a template to create specific guidance for charities on PIAs.

29. It appears that some fundraisers take the view charities are different from commercial organisations and deserve to have an exemption from the marketing rules. In our experience members of the public do not differentiate when it comes to nuisance calls or texts. It would be very welcome if the charity fundraising sector acknowledged these public concerns and were fully committed to complying with the law. It would also be very helpful if self-regulatory bodies in the sector joined in the multi-agency efforts to tackle the problem of nuisance calls.

[3] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

What the law says **Annex**

30. Directive 95/46 EC (the Data Protection Directive) makes specific provision for rights for individuals in relation to direct marketing. It also makes clear at recital 30 that the provisions relating to marketing should apply whether that marketing was 'carried out commercially, or by a charitable organisation or by any other association or foundation, of a political nature for example'.

31. The right afforded to individuals in relation to direct marketing as well as the definition of what constitutes direct marketing are found under section 11 of the Data Protection Act 1998 (the DPA). Broadly speaking, an individual is entitled to request in writing that, at the end of such period as is reasonable in the circumstances, a data controller stops, or does not begin, processing their personal data for the purposes of direct marketing. The right is absolute in that there is no test of reasonableness or necessity or prejudice when it is exercised. If a data controller receives a written section 11 request then they **must** cease processing that individual's personal data for direct marketing purposes. There are a small number of exemptions, such as the national security exemption at section 28, which can exempt processing from the right afforded under section 11. However, in the vast majority of cases these exemptions will not be applicable.

32. Section 11 also defines what is meant by the term direct marketing:

    'In this section, direct marketing means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.'

    It is clear, by virtue of recital 30 to the DP Directive that this definition must be given effect so as to include the activities of charities, political parties and other 'non-commercial' bodies. To that end, the ICO takes the view that the definition will include the promotion of an organisation's aims or ideals.

33. Regulation 21 of the Privacy and Electronic Communications Regulations (PECR) says that unsolicited live marketing calls must not be made to numbers registered on the Telephone Preference Service (TPS) unless the subscriber has notified the caller that they do not, for the time being, object to those calls being made. In short, a subscriber listed on the TPS must give their prior consent to receive the call.

34. Direct marketing under the PECR is subject to the same definition as under section 11 of the DPA. Consent is not defined in either PECR or the DPA. However, it is defined in article 2(h) of the Data Protection Directive:

'The data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'

From a marketing point of view, in practice this choice often manifests as either ticking a box to 'opt in' to marketing or not ticking an 'opt out' box. The ICO takes the view that providing an un-ticked opt in box is best practice. Our Direct Marketing guidance recognises that, under the current definition of consent, an unchecked opt out box could be sufficient to demonstrate implied consent. However, it also makes it clear that where organisations are relying on implied consent, it is even more important that the information they provide to individuals about what information they are collecting and how it will be used is clear, prominent and easy to understand. In particular, for consent to be valid it must be clear to the individual what they are consenting to. So, it must be clear to the individual that by submitting the online form and not checking the opt-out box, they are consenting to have their details used for marketing purposes. It must also be made clear to the individual who will be marketing them and by what means, either electronic, postal or both.

35. The provisions of the DPA should assist organisations with complying with the requirements of PECR. The most relevant of the DPA's requirements is principle 1 which requires, amongst other things, that personal data is processed fairly. As part of ensuring that personal data is processed 'fairly', organisations are required to provide 'fair processing information to individuals. This should explain:

    - Who the organisation is that is collecting the personal data
    - What they will do with the personal data, and
    - Any other information necessary in the circumstances to ensure processing is fair

    The third point is important in a marketing context. This is because if an organisation is intending to use the personal data they collect for marketing purposes (in addition to whatever other purposes they had collected it for) then this is the part that would require them to tell the individual. If they intend to market individuals via means which fall under PECR, then they should also as part of the fair processing information seek the individual's consent to do so.

36. It is also important to bear in mind that the General Data Protection Regulation (the GDPR) currently being negotiated in Europe is likely to alter the landscape again. While the specifics are still yet to be finalised, it is possible that the GDPR will move to an explicit consent model which must be verifiable by a data controller. The negotiations are currently at trialogue stage, the aim is to reach agreement by the end of 2015, with a

two year period for implementation, with the Regulation likely to be in-force by 2018. The ICO has been supportive of the move to a single standard of explicit consent.

37. In practical terms this means, to use current examples, that consent would only be valid if the individual had ticked an opt-in box. The current means of obtaining implied consent by providing an opt-out box which the individual fails to check would be unlikely to be acceptable to satisfy the requirements of the GDPR. While other means of obtaining explicit consent may be available they will be far narrower.

38. The ICO is in the process of developing further guidance that is relevant to direct marketing. The ICO Code of Practice on privacy notices will be revised and issued for consultation in October and the further guidance will issued in response to recommendations 5, 6 and 7 of the Which? nuisance calls taskforce on consent and lead generation[4], that will include recommended standard wording for SMEs and charities.

August 2015

[4] http://www.which.co.uk/documents/pdf/nuisance-calls-task-force-report-388316.pdf