PROTECTING YOUR BENEFICIARIES, PROTECTING YOUR ORGANISATION

Ten considerations for charities on safe use of personal data

Tracey Gyateng, Data Labs Project Manager

September 2015

Data protection is a mission critical element of daily business for all organisations—and charities are no exception. As public interest in data security grows and ever-tighter regulations on personal data are introduced, charities can't afford the risk to their reputation—not to mention the potential harm to beneficiaries—of a serious data handling mistake. However, it is also increasingly vital that charities make decisions and design interventions based on the most up-to-date evidence available. Using both qualitative and quantitative data is essential to this.

This short guide aims to introduce non-specialists to UK data protection regulations, risks and good practice—as well as pointing to trusted sources of further information and training.

The world we live in is increasingly data driven. Data is being collected constantly from individuals through daily transactions and mobile phone use, online services and loyalty cards. It is usually service providers such as businesses, governments and charities that are responsible for this data. At the moment, there is a high-profile debate over the rights of individuals; over the access and control of the data held about an individual[1]; and about who can make use of this data and for what purposes.

Currently, the key data protection and usage principles in the UK are enshrined within the UK's Data Protection Act (DPA) 1998[2]. The DPA provides guidance on how personal data should be collected, retained, used and disclosed. The EU General Data Protection Regulation (GDPR), which is expected to come into force in 2018, is likely to strengthen data protection further[3]. Ahead of these changes, all UK-based organisations will, as a first step, need to examine their compliance to the DPA. Organisations should also actively explore which personal data, both qualitative and quantitative, it is really essential to have[4].

[1] Such as the use of personal data stores, see the Mydex website for more details.

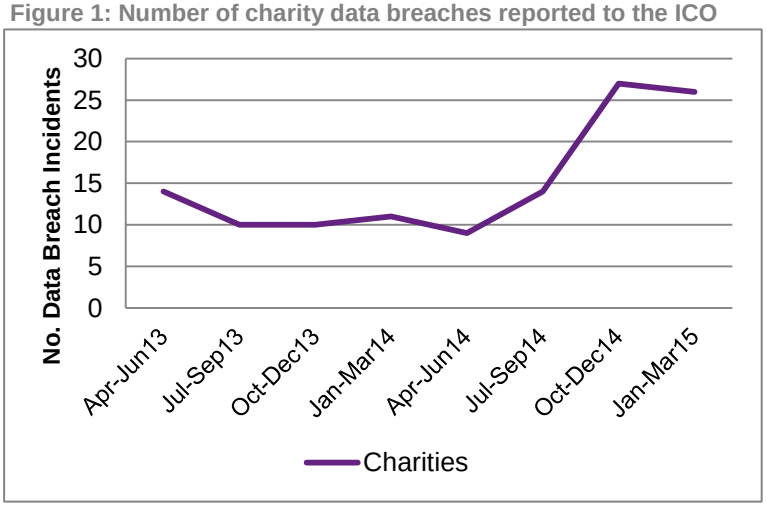
[2] Supplemented by the Privacy and Electronic Communications (EC Directive) Regulations 2003.

[3] The EU Data Protection Regulation aims to harmonise and update the data protection legislation of individual states across the EU to work within globalisation and new technology as well as to strengthen individuals' rights. As yet, it is still unclear what the impact of the new regulation will be, but a decision is expected at the end of 2015, with implementation expected in 2018.

[4] NPC's data labs project supports charities to access government administrative data to evaluate interventions. The Justice Data Lab has already been established, and is a secure 'safe setting' where personal data is provided to the Ministry of Justice (MoJ), which analyses the re-offending rates of an organisation compared to a matched control group, providing clear analytical reports back to the organisation (therefore no personal data ever leaves the MoJ). The MoJ does not retain the personal data after it has been processed nor does it use the personal data for any other purpose.

The number of breaches of DPA principles reported to the Information Commissioner's Office (ICO) is on the rise, and breaches involving the charity sector have increased sharply too as figure 1 shows. The overall number of data breaches reported to the ICO in 2014/2015 increased by 16% compared with 2013/2014. In the same period, the number of charity data breaches increased by 69%. In fact, the charity sector recorded the fourth highest number of breaches after the health sector, local government and education in the last quarter of 2014/2015[i].

Figure 1: Number of charity data breaches reported to the ICO



Source: ICO, Data Breach Trends

Most charities have limited resources for implementing data protection regulations. They need to make all their resources count. This paper highlights ten considerations for charities about making use of service users' personal data. These are based on the eight DPA principles below. This is meant as an introduction to the key issues. As you make your own plans, please refer to the full guidance on the ICO website.

Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

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

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

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

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

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

1. Understand what personal and sensitive data you hold

Let's start off with some definitions[ii]:

***Personal data** means data which relate to a living individual who can be identified—(a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.*

Data Protection Act 1998, Chapter 29 section 1

Personal data is about living people whose information is stored as 'data'[5] (dead people are not covered). Even if the data doesn't directly identify a person, it is still considered to be personal data if auxiliary information is (or is likely to be) provided that can enable the person to be identified. For example, Transport for London (TfL) was criticised for releasing journey data for people using 'Boris Bikes'[iii]. Although personal details such as names were not released, the dataset held unique customer identifiers, which meant that the journeys of people whose data had, in theory, been anonymised could be tracked. In reality it would be difficult to identify everyone who used the bike hire scheme, but creatures of habit could potentially be identified from the information given. TfL responded by immediately removing the dataset and reviewing its content before re-publishing the data without unique customer IDs[iv]. The lesson for other organisations is that it is possible to anonymise information and to make it 'safe' for release. However, there can be risks when dealing with information derived from individuals' personal data.

To process personal data, the eight principles of the DPA need to be adhered to (see page 1). Principle 1 states that personal data should be processed fairly and lawfully. This means charities need to be transparent about the information they collect and how they use it, and they must have a 'legal basis' for processing this data. In addition, at least one of the conditions under Schedule 2 of the DPA (a checklist to justify whether data can be processed lawfully) must be complied with[v]. A further requirement (Schedule 3) is placed on sensitive personal data—information considered to be sensitive because it could lead to discrimination or other forms of negative treatment[6].

Do you hold this type of data? And if so, do you know where it is stored? The British Pregnancy Advisory Service was fined £200,000 by the ICO after a hacker was able to steal personal data from the charity's website. Although this was primarily a security breach, it is important to note that the charity was unaware that its website stored the data of individuals who contacted them, enabling the data loss to occur[vi]. Many charities may be in a similar position, especially if their IT systems are outsourced. Whatever the arrangements, it is the charity's responsibility to ensure that personal data is collected and stored securely.

Do you know where personal data about your beneficiaries is stored?
If you outsource your IT services, you should ensure that contracts with IT suppliers are clear on what and where personal/sensitive personal data is collected and make sure that this data is stored securely.

[5] Data means information that is: processed electronically; recorded with the intention of electronic processing; recorded as part of a relevant filing system (which also has another definition).

[6] This information includes: racial or ethnic origin; political opinions; religious beliefs or other belief systems; being a trade union member; physical or mental health; sexual life; or criminal history.

2. Ensure people know about what happens to their data

Principle 1 of the DPA requires data controllers to act fairly and lawfully. Acting 'fairly' means letting people who use a service know who controls their data and for what purposes. Typically, this requires data subjects to have received a fair processing/privacy notice that outlines this[7].

Collecting consent from service users and providing privacy notices of what will happen to their data can often be done at the same time. However, there are two separate mechanisms for making service users aware of how their data can be used. Which method you use depends on the intended use of the data. It would be unfair if data you had collected as part of operating your services was then used for fundraising purposes. Clearly, in this situation consent would be needed. Consent is required (either via opt in or opt out) when undertaking direct marketing to service users[8].

Many charities collect consent from service users, but are these consent forms fit for purpose? It is important to check. Charities should be clear with service users that personal data may be used for research purposes—ie, shared with other organisations strictly for research and statistical purposes only. We have seen a few examples of charities wanting to undertake further analysis of service users' data. However, after reviewing their consent forms, they have realised that consent was only collected for a specific purpose, with strict prohibition of sharing their data, or using it for any other purpose other than providing a direct service. Making use of data where the consent form explicitly rules out further usage would be unfair to the data subject, and would possibly be in breach of the DPA Principle 2—ie, that personal data must be obtained for a specified and lawful purpose and should not be processed for any other incompatible purpose. A good rule of thumb is that 'incompatible' means information use that is 'different' plus 'bad'. In these circumstances, if an organisation wanted to make use of this data, it would need to write a privacy notice alerting clients to the change of use for the collected data.

The example of what happened with the Samaritans' Radar app is a good lesson in this area. The app was created to alert Twitter users of anyone they followed who may be feeling vulnerable. This was a worthy idea, but one that breached Principle 2. The app used personal data collected from individuals' tweets for a different purpose than the Twitter user originally intended. An outcry greeted the launch of the app and Samaritans suspended it within a fortnight. While it could be argued that, by posting public comments on Twitter—an open and public platform—a Tweeter has no right to object to their data being used for a different purpose. However, many people thought that the app crossed the 'creepy line' of taking data and reusing without permission. Charities need to develop a keen understanding of where their clients' sensitivities lie and what kinds of information use they would find reasonable and acceptable. If in doubt, ask some of them.

Charities rely on their service users' trust, and so it is imperative that charities are open and honest about what happens to service users' data.

For help in writing a privacy notice, please see ICO guidance on Privacy notices code of practice[vii].

[7] See ICO guidance for examples of good and bad privacy notices here.

[8] The Privacy and Electronic Communications Regulation (PECR) sits alongside the Data Protection Act and regulates how organisations should communicate with people. The ICO provides guidance and examples of how to adhere to PECR here.

3. You don't always need people's consent

Service users should always be clear about how their data will be used. Collecting consent from service users is often viewed as the most ethical basis for using personal data. However, this can sometimes be difficult for some client groups. For example, people who are homeless may have problems trusting authorities due to previous negative experiences, and are therefore less likely to grant consent for their data to be shared. With frontline staff rightly wanting to concentrate on providing care, anything that may prevent them from doing so may be resisted.

What should happen in these situations? Certainly clear explanation of how data will be used is needed. However, collecting consent from a service user is only one of several options provided in Schedule 2 (and Schedule 3 for sensitive personal data[9]) for lawfully processing data. Under Schedule 2, data can be processed where:

1. The subject has given consent.
2. It is necessary as part of, or entering a contract between the organisation and data subject.
3. It is necessary for a legal obligation (other than a contract) that may have been placed on you.
4. It is necessary for protecting the 'vital interests' (life or death) of the data subject (eg, need to disclose data to enable health treatment).
5. It is necessary for the administration of justice, houses of parliament, statutory obligations/crown, minister of the crown or government department/functions of a public nature for the public interest.
6. It is necessary for the legitimate interests of the data controller or third party or parties where data would be shared unless the processing is unwarranted or may prejudice the rights and freedoms or legitimate interest of the data subject.

The 'legitimate interests' condition can serve as a useful alternative when obtaining consent would be impractical. In short, this means that a charity can usually process clients' personal data to carry out the charity's legitimate aims, provided that the processing does not harm the client's own interests. For example, a charity wishing to use personal data to evaluate a programme could argue that it is within the legitimate interest of the organisation to provide an effective service to service users.

Further exemptions for using data without consent can be found in the DPA. One such exception is that personal data can be used for research purposes where the research is not used for targeting individuals or is unlikely to cause substantial stress or harm (DPA Section 33(2))[viii]. An example would be NPC's Data Labs project, where personal data is used to understand the aggregate effect a service has on social outcomes, with no individual data reported. (The Justice Data Lab is now a permanent service at the Ministry of Justice, and was developed by NPC).

It is important to stress that the DPA does not apply to anonymised datasets. So if you are undertaking research using personal data, an important first step is to anonymise the data[ix] (or make use of anonymous data), wherever possible, to avoid or reduce the DPA procedures required.

[9] There are further obligations for processing sensitive personal data. See the ICO website for further guidance.

4. Check whether the data you hold is needed

A quick tip: if you are a hoarding type, be aware that this is an unhelpful tendency when it comes to dealing with personal data. Incorrect use and disclosure of this data could cause your organisation harm. It is good practice to review the data you keep on a regular basis. If you have no need for the data, why hold on to it? Instead look for secure methods for deleting any personal data you hold (see point 6 below).

Certain liabilities occur when holding vast historical and unused data—such as having to grant people access to potentially redundant records if this is requested (subject access, see Point 7). However, there is no reason to delete records prematurely if you have a legitimate business need to retain the information.

5. Ensure the data you hold is accurate and kept up to date

All organisations that have a sizeable client database will understand the importance of keeping contact data as up-to-date as possible. Redundant contact information is unhelpful (and is likely to drive the organisation's communications and fundraising teams crazy!). While it is not practical to check every record for inaccuracies, it can pay off to check for accuracy when personal data is first entered or recorded in a database. Records should be updated as needed—when things change or when inaccuracies become apparent. A client may alert you to a change of telephone number or they may dispute the content of a record. If the client is right, you should amend the record accordingly. If you are not sure whether the information is right or not, as in the case of a dispute, you should either delete the information or put a note on it saying the client disagrees with what the record says.

6. Securely remove personal data that is no longer needed

The DPA does not offer any recommendations regarding minimum or maximum length of time to retain personal data. It comes down to each organisation's judgement and needs. If you retain the information for too short a time, you may not be able to deliver a service effectively. On the other hand, if you keep information for too long, you run the risk of breaching the DPA's data principles. It is a difficult call to make, but having a clear theory of change[x] defining the outcomes you want to achieve can help. For example, a charity providing intensive educational support to children through their early years should expect to hold on to data for several years so it can measure the impact when the children they have supported take their GCSEs. For a charity providing a non-intensive after-school activity, however, a more immediate impact may be anticipated and the data should therefore be retained for a much shorter period.

Once the decision to delete records is taken, organisations need to think carefully about how this is done. Deleting a database from a folder is insufficient, as the data will almost certainly be stored in the background. As long as reasonable steps are taken to delete personal data safely, such as those outlined by the ICO[xi], charities should feel they have acted appropriately. If data is actually held irretrievably on a back-up system somewhere, where there is no intention to access it, the ICO is likely to view that this puts it outside the normal data protection rules.

The ICO outlines a number of methods for deleting data: physically destroying the media (eg, memory stick on which the data was held); using secure deletion software; restoring devices back to the factory settings; accessing specialist deletion support/advice; and reformatting devices. The pros and cons for each type of deletion are provided on the ICO website.

7. Respect the right of users to object to how data is used

When it comes to data, an individual's wishes should be respected. Data subjects have the right to a copy of the information that is held about them, and while the powers to stop their data from being used can be weak in some aspects[10], there is strong protection preventing direct marketing using a subject's data. This is enshrined in the Privacy in Electronic Communications Regulations (PECR). The case of Olive Cooke, who felt pressurised by the number of donation requests made by charities, has recently shone a light on the practices of fundraisers. Several charities have been investigated to see if they were in breach of PECR by contacting people who had opted out of Telephone Preference Service (TPS), which bars unsolicited sales calls. Charities need to be aware that clear consent, with either opt in or opt out in terms of marketing materials, should be applied and actioned. Individuals' wishes when it comes to marketing calls and other approaches must be respected.

Many private sector organisations make use of lengthy terms and conditions for using their service as a way of weakening the rights of service users. They know that very few people can be bothered to read the legal wording before downloading new apps or using online services. An often-cited example was the terms and conditions devised by GameStation for an April fool's joke. GameStation changed the terms and conditions of their service to include a clause that the company would own the purchaser's soul. Only 12% of customers refused, indicating that either people were happy to give up their soul for a computer game, or that they didn't read the terms and conditions! The charity sector should aim to do better, and to be as transparent as possible. We should make people aware of how their data is going to be used, even if we may suspect that many people are not overly concerned.

Most service users do not want to read long, complicated terms and conditions. We should work to be as transparent as possible, tailoring our conditions so they are in line with people's expectations.

If a service user has an objection about their personal data, take it seriously, look into the issue, and be prepared to change the way you do things if necessary. Regard it as a learning experience and as a way of developing a better service.

[10] Individuals' rights under the DPA are limited. For example, people do not have the right to order you to delete their information just because they want you to.

8. Ensure that staff and systems process data safely and securely

Safe handling of data is essential for data-holding organisations. Loss or theft of unencrypted data accounts for 40% of the ICO's undertakings and fines, according to data watchdog Breach Watch, while 50% of fines were related to insufficient staff training on handling personal data[xii]. There have been high-profile cases in the public sector of unencrypted laptops or memory sticks with personal data on them being left on trains. The charity sector has not emerged unscathed from damaging data loss. For example, both Asperger's Children and Carers Together (ACCT) and Wheelbase Motor Project had unencrypted personal data stolen from computers.

Breaches have also occurred through staff being unaware of data protection procedures. In one case, a member of staff at Foyle Women's Aid took excessive information out of the office (ie, information not relevant to the meeting) which was subsequently left behind in a cafe[xiii]. Implementing clear data protection guidance and training is imperative if an organisation is to adhere to the DPA and to avoid any data leakages. It is good practice for a nominated person within an organisation to have responsibility for data security (for example, a data protection officer) and that they report to senior management.

Charities need to be particularly careful to make sure that employees or volunteers who work from home, travel or use their own equipment adhere to all of the organisation's security rules. If in doubt, consider prohibiting these activities. Data breaches are messy and expensive to clear up. They could mean that you have broken the law and so are best avoided in the first place.

An organisation must understand:

- what personal data is stored and where; and should ensure it is protected using up-to-date security measures;
- that staff are trained in complying with data protection procedures/policies; and
- that there is an understanding of the likely harm that could occur if personal data was misused or lost (undertaking a privacy impact assessment can be useful for identifying and reducing potential risks).

9. Know which country your data is stored in

The use of cloud computing has increased rapidly due to its relatively low cost and convenience compared to traditional methods such as local servers. However, organisations need to be mindful of where any data placed on the cloud is stored.

Personal data should not be transferred outside of the European Economic Area (European Union plus Iceland, Liechtenstein and Norway) unless the country or territory has adequate levels of protection for personal data.

Speak to your cloud service providers about where data is stored. There are, however, exemptions so reading the ICO guidance[xiv] is recommended.

10. If in doubt, ask for help!

This paper has highlighted key areas for consideration when processing personal data, but it is **not** a substitute for understanding the DPA in full. For those without a technical or legal background, the DPA landscape can appear to be quite complicated and difficult to understand. If you're in this position then it might be helpful to find out from similar organisations what their procedures and protocols are.

Otherwise, infrastructure bodies may be able to help. For example, the Small Charities Coalition provides a list of organisations where *pro bono* legal advice can be sought and DSC offers data protection guidance. Attending a data protection course can also be useful—Amberhawk's certificate in data protection is one of many available.

Finally, don't forget you can always consult the ICO, which is keen to offer charities support on the collection and use of service user data. The ICO website hosts a variety of guidance to help organisations navigate the DPA. Contact them if you need advice about any personal information issues. They offer free one-day advisory visits to charities and are particularly keen to reach out to charities' representative bodies, so hopefully more detailed general guidance for charities will be developed in the future.

However you choose to learn about data protection, our advice is to do it soon before any mistakes or breaches occur. Awareness and training on data protection should certainly be part of any strategy related to a charity's use of digital technology.

Acknowledgements and contact details

Thanks to Chris Pounder of Amberhawk and everyone who reviewed this paper: Iain Bourne and Sara Rolin, ICO; Libby Bishop, UK Data Service; Emma Prest, DataKindUK; and colleagues at NPC. All errors remain the author's responsibility.

If you have any questions, please get in touch via info@thinknpc.org and visit www.NPCdatalabs.org.

Useful links

[i] https://ico.org.uk/action-weve-taken/data-breach-trends/

[ii] https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

[iii] http://qz.com/199209

[iv] http://www.buzzfeed.com/sirajdatoo/tfl-has-been-accidentally-allowing-anyone-with-a-computer-to#.hrJqEz6eY

[v] https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/

[vi] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/03/british-pregnancy-advice-service-fined-200-000/

[vii] https://ico.org.uk/media/for-organisations/documents/1610/privacy_notices_cop.pdf.

[viii] http://www.academia.edu/1321926/Section_33_of_the_Data_Protection_Act_1998_a_practical_note_for_researchers

[ix] https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/

[x] http://www.thinknpc.org/publications/creating-your-theory-of-change/

[xi] https://ico.org.uk/for-the-public/online/deleting-your-data/

[xii] http://breachwatch.com/about/

[xiii] https://ico.org.uk/action-weve-taken/enforcement/foyle-womens-aid-follow-up/

[xiv] https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

TRANSFORMING THE CHARITY SECTOR

NPC is a charity think tank and consultancy which occupies a unique position at the nexus between charities and funders, helping them achieve the greatest impact. We are driven by the values and mission of the charity sector, to which we bring the rigour, clarity and analysis needed to better achieve the outcomes we all seek. We also share the motivations and passion of funders, to which we bring our expertise, experience and track record of success.

Increasing the impact of charities: NPC exists to make charities and social enterprises more successful in achieving their missions. Through rigorous analysis, practical advice and innovative thinking, we make charities' money and energy go further, and help them to achieve the greatest impact.

Increasing the impact of funders: NPC's role is to make funders more successful too. We share the passion funders have for helping charities and changing people's lives. We understand their motivations and their objectives, and we know that giving is more rewarding if it achieves the greatest impact it can.

Strengthening the partnership between charities and funders: NPC's mission is also to bring the two sides of the funding equation together, improving understanding and enhancing their combined impact. We can help funders and those they fund to connect and transform the way they work together to achieve their vision.

New Philanthropy Capital
185 Park Street, London SE1 9BL
020 7620 4850
info@thinkNPC.org

Registered charity No 1091450
A company limited by guarantee
Registered in England and Wales No 4244715

www.thinkNPC.org