Bates Wells

CHARITIES GOING DIGITAL

Top 10 Data Privacy Tips

Certified B Corporation

www.bateswells.co.uk

Introduction

There has been a widespread and **well documented** increase in innovation and invention through the charity sector as a result of Covid-19. That trend is expected to continue through 2021 among charities and in other sectors. One key finding in that report was that seven in ten charities want to make more services digital and deliver new services remotely over the coming year.

Data protection compliance needs to be built into the design of any new technology and data processing systems and should not be an afterthought. Here we have flagged 10 top data protection tips for charities which are moving into new digital ventures.

In this guide references to the GDPR are to the General Data Protection Regulation (EU) 2016/679 as implemented into UK law.

For more advice on data protection compliance and use of new technologies or digital services contact
Mairead O'Reilly
m.oreilly@bateswells.co.uk

#1 Do your due diligence when choosing a technology provider

When choosing suppliers to build or support a new platform or provide a new service, it's important to ask the right questions. In many cases these suppliers will be acting as processors on behalf of your charity. This means that in most cases the charity which is commissioning the service will be ultimately responsible for any breach of data protection law by those suppliers. The GDPR only permits the use of processors which provide sufficient guarantees that they will implement appropriate security measures to ensure their processing meets GDPR requirements. For this reason it's important for charities to:

- Research potential suppliers carefully;
- Consider their market reputation and ask for evidence of their GDPR track record;
- Document any due diligence you have undertaken on them; and
- Ensure that regular service reviews are carried out to revisit supplers' data protection compliance over time.

#2 Get supplier contracts correct from the start

If your supplier is a processor, you'll need to have an agreement with them that complies with the requirements of Article 28 GDPR. Many suppliers will have their own standard data processing agreements but remember – as a controller you are required to ensure that the agreement is compliant.

If your suppliers are based overseas, it will be necessary to consider how to comply with the data protection restrictions on international data transfers. For transfers to suppliers outside the European Union, you will need to check whether the supplier is based in a country which has been designated as providing adequate data protection.

Countries which currently have adequacy findings include Argentina, Israel and Switzerland. For transfers to countries which have not been deemed adequate (for instance India or the USA) you may need to enter into standard contractual clauses in addition to or as part of your service agreement with your supplier. The law relating to these clauses has recently become more complex following a decision of the European Court of Justice (Schrems II) and the publication of draft updated standard contractual clauses by the European Commission in December. For more information on this area see this **recent article** by Victoria Hordern.

#3 For new projects or services involving the use of personal data, do a Data Protection Impact Assessment (DPIA)

Article 35(1) GDPR says that you must do a DPIA where your processing is likely to result in a high risk to the rights and freedoms of individuals. The ICO cites a number of examples of processing that is likely to result in a high risk. Included in that list is *Innovative technology: processing involving the use of innovative technologies, or the novel application of existing technologies (including AI).*

If in doubt, where the new digital venture that you are considering involves the use of personal data of supporters or others in a new way, do a DPIA!

A proper risk assessment of a new technology requires a deep understanding of the impact that the new technology or service will have on individuals' data protection rights so a DPIA needs to be carried out by someone who understands the technology and how it will impact on the use of personal data!

#4 If your digital project involves sharing data with partners and others who will act as separate controllers, consider whether you need a data sharing agreement.

Using tech in a new way can often involve sharing data with partners or other affiliated entities, for instance a charity may decide to share personal data with its trading company and other related entities via a shared database. When entering into new regular data sharing like this, it's helpful to consider the ICO's new **Data Sharing Code of Practice**. While data sharing agreements between controllers are not mandatory, the Code advises that having one can help organisations to demonstrate that they're meeting their accountability obligations under the GDPR.

#5 Tell people if there will be a change to how you process their personal data! Is your privacy notice up to date?

If you're entering into a new digital venture, consider whether this will result in you doing something new with the personal data of your supporters, members, staff or others. Are you sharing data in a new way or seeking to use the data that you hold for new research or analysis purposes? Will you be promoting a new service to individuals? If you're using individuals' personal data for a new purpose, you will need to update your privacy notice and bring any changes to your privacy notice to the attention of individuals. Some changes to how you process personal data (for instance, to use data for fundraising purposes) may also require you to obtain prior consent from the individuals whose personal data is being processed for this new purpose.

#6 Be extra careful with children's data – especially if you will be marketing to them and don't forget about the new Children's Code

If you will be using children's data as part of your new digital initiative, remember that children's personal data demands extra protection under data protection legislation. The GDPR prescribes that where organisations are offering certain online services directly to children in the UK and relying on consent as their lawful basis in the context of providing those services, the consent of a parent or someone with parental responsibility is needed for children who are under the age of 13.

This does not mean that controllers always need consent to process a child's personal data when providing online services to them. In most cases it will be easier to rely on an alternative lawful basis for processing a child's personal data under the GDPR, such as legitimate interests. However, in some cases consent will be needed, for instance to send marketing emails and texts to a child.

The ICO requires organisations to carry out a DPIA when they are profiling children or targeting them with marketing or online services and has produced a template DPIA for use when providing online services likely to be accessed by children.

Finally, if you're engaging with children online, it's important to be aware of the Age Appropriate Design Code (also known as the Children's Code) – a statutory code of practice published by the ICO and designed to ensure that online services safeguard children. You can read more about the Code **here**.

#7 Keep personal data secure

A key principle of the GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures'. When using new technologies this may involve carrying out risk analysis, introducing organisational policies as well as physical and technical measures to protect personal data. The measures that you implement to protect personal data should be proportionate to the risk posed by that processing. This obligation together with the obligations to notify certain data security breaches within 72 hours means that new technologies should be designed to prevent breaches where possible, detect them and make it easier for your organisation to respond to breaches when they do happen. Even if you are satisfied that a new system offers good protection, it is important that you regularly test, assess and evaluate the effectiveness of those systems.

#8 Take stock of what you're doing on your website with cookies and trackers

Many organisations are investing in new websites or enhancements to their websites as their presence online becomes more important in the absence of physical connections. It's important for charities to understand what cookies and other technologies are being used on their websites. Many do not have clear enough oversight over which cookies they're using and why. The law relating to cookies requires organisations to obtain consent for the use of non-essential cookies. Although historically compliance with the rules on cookies has not been a regulatory focus of the ICO, there is increasing evidence of public scrutiny of the use of invasive cookies (including by charities) by data privacy pressure groups and others. Therefore there is a reputational risk as well as a regulatory risk associated with not engaging with these rules.

#9 Fundraising through social media

With the reduction in opportunities for face-to-face and other traditional methods of fundraising, more and more charities have been using the fundraising tools available on Facebook and other social media platforms to improve their reach. When grappling with the laws around tools such as lookalike audiences, remember the data protection principles are the same regardless of how elaborate the mechanism for targeting supporters is.

For instance, if you are using social media tools for the first time it's likely that you will need to update your privacy notice to explain to individuals that you are sharing their data with social media platforms for these purposes. It may also be necessary to obtain consent to the sending of fundraising messages via social media. The ICO produced a **draft Code of Practice on Direct Marketing** in March 2020 and, as part of that, considered the use of social media marketing tools. Publication of the final Code is awaited later this year.

#10 Protecting data protection rights

For organisations which plan to move or consolidate large quantities of personal data onto new platforms or systems, it's important to assess whether these new systems will make it easier for your organisation to comply with requests by individuals to exercise their data protection rights (such as the rights of access or to rectification). A well designed system can transform an organisation's ability to respond to a data request. Therefore it's important to assess how easy your new system makes it for you to:

- categorise personal data;
- search and retrieve information;
- redact data;
- effect suppression requests; and
- allow for easy transmission of information with other organisations where necessary.

Bates Wells

Making a profit is core to all businesses but our goal is to combine this with a real social purpose. Our values are important to us, they shape our decisions and our working life.

Since opening in 1970, we've focussed on positive social impact as much as we have on being a successful law firm and we were the first UK law firm to achieve B Corp certification.

Today, our clients are diverse – from corporate household names, to public bodies, to start-ups. We're also the firm of choice for thousands of charities and social enterprises. We continue to lead the market we helped to shape.

As a purpose and values driven firm we show commitment to our clients, our people, the environment and society. We see it as our purpose to create a positive impact. The impact we have on our people, our communities and our planet does more than inform our work – it gets us up in the morning.

Bates Wells challenges what is possible in legal expertise delivery.

Get in touch:
+44(0)20 7551 7777
hello@bateswells.co.uk

www.bateswells.co.uk