GDPR: Is your charity ready? Savoo's 8 step checklist to compliance

GDPR - four letters which you'll be all too familiar with by now. With some weeks left until the regulation comes into effect, it's now more important than ever to take the necessary steps to make sure you're in line with the new rules. Online fundraising and voucher code platform Savoo.co.uk has a useful checklist for your charity's GDPR strategy.

To refresh your memory, the General Data Protection Regulation - or GDPR - will come into force on 25th May after four years of deliberation. Its main aim is to make it easier for consumers to control how their data is used by companies. Therefore, any organisation that holds consumers' personal information - names, email addresses, bank details, for example - must collect consent from the consumer about what they can use and how they can use it. And that includes all charities, regardless of their size. Essentially, it means organisations will have to become more transparent.

It may have been deemed the biggest shake up of personal data privacy rules since the birth of the internet, but what does GDPR mean for charities? Despite the Code of Fundraising Practice being updated to include new sections on personal information and fundraising, content of fundraising communications, and emails, the Direct Marketing Association has stated that 72 percent of organisations in the UK feel merely 'somewhat prepared' for GDPR coming into force.
With a hint of uncertainty lingering in the air, now's the time to make sure you're all set for the 25th with these last-minute checks.

1. Do you know which data you currently hold?

As with any task, it's crucial to figure out what you're working with before you can put any effective actions into place. Carrying out a data audit will give you a clearer picture on what kind of data you already hold, what you will continue to hold moving forward and what data you have no use for. Plus, it's an opportunity to reconfigure the process of how you collect data, how it is stored and who has access to it.

After 25th May, it's against the law for any organisation to hold data they don't need, so use this as a chance to clear up your database. Depending on when you last took a look at your databases, this will be a useful exercise in any instance.

2. Have you reviewed how you ask for consent?

It will no longer be sufficient to simply include a link to your privacy policy when asking for data from your supporters and donors. When an individual shares personal data with your charity - whether that's for fundraising or communication purposes - asking for consent and the reasons why you're asking for their details and what you will be using them for needs to be clear, concise and unambiguous.

Email: ChristieDay@savings.com **Twitter**: @Savoo **Facebook**: www.facebook.com/savoo.co.uk

GDPR applies to existing data too; it's not just a case of creating a new database for new data. You must ensure all of the data you're holding has been consented to. When it comes to communications, an 'opt in' rather than 'opt out' capture method of consumer data is strongly recommended; the regulation itself states specifically that 'silence, pre-ticked boxes or inactivity should not constitute consent'. Double opt-in - that is a tick box as well as a verification email - is not necessarily a GDPR requirement but is certainly recommended practice when collecting new data. Remember that any data you do not have consent for must be deleted completely.

3. Have you trained staff members?

With stronger emphasis on a consumer's right to know where and how their data is being used, charities should be prepared for access requests from donors who may want to check the data you hold and what you do with it. It's important to have a plan in place for handling requests like this, and train staff members, workers, and volunteers accordingly to ensure data requests are handled smoothly and correctly. Bear in mind any budget or resource restraints when coming up with a plan of action.

If you haven't yet appointed a Data Protection Officer, or somebody to overlook the process at the least, now is your time to do so. You may not legally require one, but it's best practice to have an internal taskforce to monitor compliance and give advice to colleagues.

4. Do you have the correct procedures in place to detect, report, and investigate any breaches of personal data?

Under the new rules, failure to demonstrate compliance can lead to fines of up to €20 million or 4 percent of an organisation's global annual turnover profit - whichever is highest. That said, if your charity does encounter a breach of personal data, there is a duty to report certain types if they occur. Make sure your charity has the right protocols in place to detect and report a breach, as well as investigate how it happened to ensure it doesn't happen again. While fines will be the last resort in terms of punishment, the detrimental impact on your charity's name may be instant and long-lasting.

5. Is your data stored securely?

Data security plays an important role in the new GDPR regulations, and the best way to avoid sanctions is to put the correct procedures in place to prevent data breaches in the first place. If you haven't already, review your data security. If there are any doubts about your data management system, consider implementing a new, safer, data storage system. Consider any technical requirements as well as who has access to which data. Remember to document any steps you take to maintain security of the data you hold - this will help your cause should a breach occur.

6. Have you made it easy for consumers to view and manage their data?

People have the 'right to be forgotten' under the new rules. This means that, should an individual wish to, they can request their data to be removed completely from your charity database. If you receive a request like this, it's important to erase any data relating to this person that you may have stored. Depending on what kind of charity you are, this could be anything from somebody's name and address to more sensitive details such as their ethnicity, disability status, or sexual health. On a similar note, it must be easy for supporters or

donors to see what data you have relating to them, with the new regulations stipulating that their data must be provided to them, on request, in a machine-readable format. Similarly, the ability to rectify or update data preferences must also be possible at any time.

Daniel Fluskey, Head of Policy and Research at the Institute of Fundraising told The Guardian it's worthwhile considering putting a process in place, such as to include "Find out what information we hold on you" and "Remove all information about me" sections in your privacy policy to give people clear information.

7. Have you done a cookie audit?

A cookie is a small piece of code your website sends out to collect browsing data on anybody who visits your website. Cookies - whether they are deemed essential to the functioning of any website, or aren't directly fundamental to the site's functionality - will still be collecting data, so will need to be consented to by a user. Thus, carrying out a cookie audit is key. Find out what cookies you're using, why you're using them, and what kind of data they collect. If you have any you're not using, consider removing them.

You'll be aware of the standard 'By using this site, you accept cookies' messages you see pop up when you visit a website. Under the new GDPR rules, these are no longer sufficient. The IT Governance Blog states that it must be possible for consumers to opt in to give their consent to you using different types of cookies, as well as opt out to reject cookies. Consider revising your cookie policy to ensure compliance.Bear in mind that the individual has the right to withdraw consent at any stage, so you must make it possible to do so.

8. Are you keeping up with the latest GDPR developments?

While the final Information Commissioner's Office (ICO) guidelines have already been published, the last eighteen months have proved that developments in GDPR compliance and regulation interpretations are aplenty. New information quickly becomes outdated, so make sure you're up to speed with the latest rules, regulations and implications.

There are plenty of reliable resources out there for charities and GDPR, and it's worth speaking to charity partners, other charities, and industry figures to get a feel for how they're preparing for the implementation of GDPR. Hugh Radojev from Civil Society's Fundraising magazine summed it up appropriately; "this process doesn't simply end on 25th May: GDPR is a marathon, not a sprint", so staying up-to-date with developments now, as well as in the coming months, is as paramount as ever.

For Savoo's 8-step GDPR checklist in infographic format, click here.

Please note this list is not exhaustive and by no means legal advice.