RISK INSIGHTS Not-for-Profit

Crendon Insurance Brokers

GDPR Guidance for Charities

Despite the good-natured work that charities do, these organisations possess a significant risk for cyber-attacks, according to recent research from the Department for Digital, Culture, Media & Sport. In fact, nearly 20 per cent of UK charities experienced a data breach in just the past 12 months, with 40 per cent of those charities reporting negative impacts as a result.

In the era of advancing technology in the workplace and stricter data protection under the General Data Protection Regulation (GDPR), it is vital for your charity to take the threat of a cyber-attack seriously. To continue contributing to your cause and avoid costly noncompliance fines, implement the following GDPR best practices at your charity.

Fundraising Techniques

Seeing as digital communication is often the most common and convenient method for fundraising, your charity likely utilises direct marketing strategies such as emailing and texting to encourage donations.

But under the GDPR you cannot market—or process any personal data—without a lawful basis. There are six different lawful bases that organisations may claim in order to process personal data. 'Processing' means doing anything with that data—collecting, recording, storing, etc. That includes marketing. No one basis is better than the other. However, in terms of fundraising, the two most likely options for your charity include consent and legitimate interest.

- **Consent** refers to an individual freely providing specific, informed confirmation that they wish for your organisation to process their data. In order to obtain valid consent:
    - Be clear and concise when requesting permission. It is important that the individual understands what they are agreeing to.
    - Consent must be concrete and proven, such as by choosing a 'yes' option in an email or providing written confirmation through a text. If individuals must tick a 'yes' or 'no' box in an email or online, be sure your charity is asking them to opt-in (tick the 'yes' box themselves) rather than opt-out (deselect a pre-ticked 'yes' box).

In the era of advancing technology and strict data protection regulations under the GDPR, it is vital for your charity to take the threat of a cyber-attack seriously.

    - Specify why you want the data and what you're planning to do with it.
    - Give separate distinct options to consent separately to different purposes and types of processing.
    - Name your charity and any third parties who will rely on their consent.
    - Tell individuals how they can withdraw consent, that they can do so without harm and that consent is not a precondition of service.
- **Legitimate interest** differs slightly in that it doesn't require the individual to blatantly say 'yes' to

receiving communication from your charity. Rather, this method permits processing data so long as the interests of the organisation and the individual are balanced (the individual hasn't said 'no' and the strategies don't cause harm or override their privacy rights). The Information Commissioner's Office (ICO) has made it clear that direct marketing (fundraising) can be considered a legitimate interest, but it also cautions that legitimate interests is the most flexible lawful basis for processing and you cannot assume it will always be the most appropriate. It is up to you to determine whether legitimate interest applies. To help you do so, undertake the ICO's three-part legitimate interest assessment.

Handling Personal Data

Whether it be accepting donations or storing information on beneficiaries and volunteers, the GDPR emphasises the need for your charity to handle personal data in a protective manner. Charities typically possess the following personal data:

- If a charity needs to store data on a beneficiary for any reason, they likely possess **special category data** about that individual. This refers to sensitive information regarding race, ethnic origin, politics, religion, genetics, health, sex life or sexual orientation.
- When a charity accepts donations, it temporarily possesses **finance-related data** about the donor.
- If a charity has volunteers for their cause or for specific events, they likely will temporarily possess **contact information** about the individual. In some circumstances, such as a blood donation, the charity may possess **special category data** as well.

Consider the following tactics when handling this data:

- **Encryption** refers to encoding messages or private information in a way that only authorised individuals can access or understand it. With this method, even if your data is compromised, it is unlikely that a cyber-criminal will make sense of it.
- **Pseudonymisation** is a process that involves using artificial identifiers (eg using 'John Smith' rather than a real name) to protect individuals' identities. This way, if a cyber-criminal retrieves sensitive data, they won't be able to link it to an individual.

Special category data is personal data which the GPDR says is more sensitive, and so needs more protection. Click here for an overview of your extra responsibilities when processing special category data.

Creating a Proper Privacy Notice

While your charity may already possess a privacy notice, it is important to ensure it complies with GDPR guidelines. Your privacy notice should include the following information:

- Your purpose and lawful basis for data collection
- Your legitimate interests for data collection
- The categories of data you plan to collect
- Any additional recipients besides your charity of the data or potential transfers of data
- How long you intend to keep the data
- Where you store the data and how you intend to keep the data secure
- The source of the personal data
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data
- The details of the existence of automated decision-making, including profiling
- Individuals' rights regarding data collection, including the right to withdraw consent and lodge a complaint with the supervisory authority
- Your charity's name and contact information, as well as the name and contact details of your representative and data protection officer

In addition to updating your privacy notice, consider whether any associated policies, such as a data retention policy, need to be updated as well.

Trustee Liability

As a trustee, a large portion of your role includes taking responsibility for managing your charity's actions and resources. Without proper cyber-measures, you may be held accountable for your charity's mistakes. Be sure to follow these best practices within your role:

- Help develop a **cyber-risk assessment and management plan**. First, identify potential vulnerabilities and areas with the greatest cyber-risk. Then, work with your management team to create a proper prevention and response plan to a potential cyber-attack.

- Ensure that all employees at your charity understand **how to respond** to a cyber-attack. This includes informing the relevant supervisory authority within 72 hours and providing proper records of the attack. For more guidelines, click here.

The ICO's Top 5 Tips for Charities

In addition to the previous guidance, rely on the ICO's top five data protection tips for small and medium-sized charities and third-sector organisations:

1. **Tell people what you are doing with their data.** People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as an established best practice), so it is important that you are open and honest with people about how their data will be used.

2. **Make sure your staff are adequately trained.** New employees must receive data protection training to explain how they should store and handle personal information. Provide refresher training at regular intervals for existing staff. Use the ICO's charity toolkit to communicate the importance of data privacy to your employees.

3. **Use strong passwords.** There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain an upper and lower case letter, a number and ideally a symbol.

4. **Encrypt all portable devices.** Make sure all portable devices—such as memory sticks and laptops—used to store personal information are encrypted.

5. **Only keep people's information for as long as necessary.** Make sure your organisation has established retention periods in place and a process for deleting personal information once it is no longer required.

Finding Proper Cover

Remember that the GDPR emphasises transparency, accountability, and 'data protection by design and by default', so consider data protection and privacy issues in everything you do. It is important for you to ensure that all staff members within your charity, not just senior management, embody an organisational culture that places utmost value in data protection.

In addition to this mindset, you can provide your charity with ultimate peace of mind through robust cover, such as cyber-insurance and trustee indemnity insurance. For more information, **contact Crendon Insurance Brokers Ltd** today.