ADVISORY NOTE

Charities, Trustees & Data Protection July 2022

BACKGROUND

The third sector is an integral part of the UK economy. With an annual income of £56bn and employment growing faster than other sectors, this is an opportune time for charities to look inwardly on themselves in terms of their compliance with data protection legislation.

Charities can be global or national or small and focussed, providing support at a local level. No matter what their size, most, if not all, charities will process personal data whether in relation to their own directors and staff, trustees and volunteers or sponsors and donors.

To that end, charities of all sizes will need to comply with the requirements of relevant data protection legislation including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and the Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003 (PECR). Global charities will also need to comply with data protection legislation in the countries in which they are processing personal data.

DATA PROTECTION OVERVIEW

Charities have different legal structures including incorporated charities and unincorporated charities. Responsibility, and potential personal liability, will depend on the legal status of the charity, however, all charities that process personal data will be 'controllers' in terms of both the UK GDPR and DPA18, no matter what their status.

In the UK, there are some exemptions for not-for-profit organisations in terms of paying the notification fee to the ICO, but charities will still need to comply with the requirements of the relevant data protection legislation even if they are exempt from paying the fee. Limited exemptions also apply to some of the compliance requirements such as the need to maintain a Record of Processing Activity (ROPA) in accordance with Article 30 of the UK GDPR.

Data protection legislation (specifically the UK GDPR) sets out the overriding principles which underpin the framework for compliance. These include ensuring that any processing of personal data is fair, lawful, and transparent, that personal data is only used for the purpose for which it was collected, that only relevant and necessary personal data is processed, that personal data is accurate and not kept for longer than necessary, and that there are adequate security measures in place to protect the personal data that's being processed.

ACCOUNTABILITY

One of the fundamental principles to be found in data protection legislation is the accountability principle which requires organisations, including charities, to demonstrate how they comply with the requirements of the legislation. For example, a controller must engender a culture of privacy and compliance that pervades the whole organisation, instilled through a proactive training and awareness programme, and supported by various policies and procedures.

GOVERNANCE AND THE ROLE OF TRUSTEES

Good governance is equally important in terms of data protection compliance. There must be senior level buy-in, and, in the context of charities, this means trustees, directors, governors and committee members. Trustees are legally obliged to comply with charity law requirements, and other laws applicable to the charity, so compliance with relevant data protection legislation is a fundamental part of a trustees' responsibilities.

To that end, there should also be senior level oversight of data protection risks and mitigations, including, but not limited to, the signing-off of data protection policies and procedures as appropriate. Many charities have boards and committees in place that oversee data protection matters and provide senior level oversight as there is significant reputational risk when things go wrong. Accordingly, accountability sits with the charities' senior management i.e. the trustees.

Trustees may also be personally liable for any financial loss they cause or help to cause. Trustees therefore have significant responsibilities, and the Charity Commission (for England and Wales) has set out those responsibilities in detail.

DATA PROTECTION RISKS FOR CHARITIES

The ICO carried out an investigation into charity fundraising practices between 2015 and 2017, and subsequently fined 13 charities for non-compliance with relevant data protection legislation. The main issues were to do wealth screening (e.g. a lack of transparency), marketing practices and inappropriate data sharing.

Notwithstanding the regulatory action taken by the ICO, those risks remain, and charities generally need to ensure that any processing activities which involve:

- Wealth screening
- Direct marketing
- Fundraising
- Data sharing
- Day to day processing of special category data and criminal offence data

…. are compliant with the requirements of the relevant data protection legislation.

POTENTIAL REGULATORY ACTION

Trust and reputation are important and charities risk significant reputational damage if they infringe the relevant data protection legislation and become subject to regulatory action by the ICO, including, but not limited to the serving of any of the following notices:

- Information Notice
- Assessment Notice
- Enforcement Notice
- Monetary Penalty Notice

Charities are not exempt from regulatory action and numerous charities have been issued Monetary Penalty Notices [fines] for poor data protection practices. Clearly fines have a substantial impact on charities, but Enforcement Notices can be equally damaging as the Information Commissioner can mandate specific action to resolve an issue or halt processing altogether. In any event, any regulatory action is likely to lead to reputational damage and a lack of trust in terms of the charity's ability to process personal data. Other regulators can also take action when there is a data protection incident including the Charity Commission and the Fundraising Regulator.

WHAT CHARITIES NEED TO DO TO COMPLY

Many charities have worked hard to ensure compliance with relevant data protection legislation and, consequently, they will have an adequate data protection framework in place. Some charities will however be less mature and will need to address the following:

- Ensure senior level responsibility for data protection within the charity;
- Ensure that trustees are aware of their responsibilities and have been adequately trained on privacy and data protection related matters;
- Consider whether a Data Protection Officer is required or, if not, whether there is sufficient knowledge of data protection legislation and practices within the charity to be confident that all processing activities e.g. fundraising, are compliant;
- Undertake a data mapping exercise to understand and document what type of personal data is being processed, the purpose of the processing, the legal basis for the processing, who it is shared with and how long it is kept for;
- Ensure that all the relevant policies and procedures are in place and that staff/volunteers/trustees are aware of them; and,
- Ensure that processes and procedures are in place to comply with data subject rights requests such as right to be informed and right to access personal data.

INTERNATIONAL DATA TRANSFERS

Global charities and charities that transfer personal data out of the UK and/or EEA will need to ensure their processing is compliant with the relevant data protection legislation. The UK position has recently changed, and Article 46 of the UK GDPR sets out the appropriate safeguards (when transferring to a country not deemed 'adequate') and moves away from the EU version of the GDPR by introducing a new mechanism for restricted transfers which is the International Data Transfer Agreement (IDTA) and UK Addendum.

Charities can continue to enter into new contracts on the basis of the old EU Standard Contractual Clauses agreed by the European Commission until 21st September 2022 as these contracts will continue to provide appropriate safeguards until 21st March 2024. From that date, however, if restricted transfers continue, then charities will need to enter into a contract on the basis of the IDTA or the UK Addendum or find another way to make the restricted transfer under the UK GDPR such as, for example, Binding Corporate Rules or a legally binding and enforceable instrument between bodies.

CONCLUSION

Implementing appropriate technical and organisational measures will help to ensure that the charity's processing of personal data is compliant with the relevant data protection legislation. It will increase trust in the charity, and donors will be more inclined to engage with the charity and support worthy causes. It also means the charity can work towards being an exemplar of best practice in what can be a competitive sector, particularly as garnering support may be difficult at this time due to increases in the cost of living and donors potentially being more limited in terms of donations. Reducing risks of incidents and breaches occurring is fundamental to this as any regulatory action will tarnish the reputation of the charity as well as potentially having a significant financial impact if a fine is issued.

CONTACT US

Call: +44 (0) 20 7566 4000
Email: info@mooreclear.com