Rollits LLP

GDPR fact sheet for charities

GDPR fact sheet for charities

1. How is the data protection law change being implemented and when will it take place?

The General Data Protection Regulation ("GDPR") takes the form of a Regulation which is already in force in all EU member states without implementation of national legislation. Enforcement of the GDPR will not begin until 25 May 2018 and the UK's current legislation – the Data Protection Act 1998 ("DPA") – will continue in force until that date.

2. Will the proposed changes fall away when Brexit is complete?

No. Although, post-Brexit, the GDPR will no longer automatically apply in the UK, the UK will need to ensure that its data protection laws provide an adequate level of protection for personal data by EU standards. The UK has signified its intention to transpose the GDPR into national legislation through a Data Protection Bill so that the GDPR effectively continues to apply post Brexit.

3. What are the key changes?

The overarching objective of the GDPR is the same as the DPA: to protect individuals' personal data. The GDPR does, however strengthen the protection granted to EU citizens in respect of their personal data in a number of ways. For example:

Consent

The conditions for obtaining consent to process personal data have been strengthened and where charities are relying on consent they will need to be able to demonstrate that such consent was "freely given, specific, informed and unambiguous". Charities should review their current mechanisms for obtaining consent and ensure that they satisfy the stricter GDPR requirements. Charities that carry out significant public-facing fundraising and employ people, use volunteers and/or process service users' personal data will be particularly impacted.

Accountability

Charities will be required to demonstrate that they comply with the data protection principles. Charities should conduct an audit to establish what personal data they process and implement appropriate technical and organisational measures to demonstrate that data protection has been considered in respect of any processing activities (for example, by implementing appropriate data protection policies, staff training, internal audits and reviews of HR policies). Some charities will be under an obligation to appoint a data protection officer, and data protection impact assessments will be compulsory in certain circumstances.

Individuals' rights

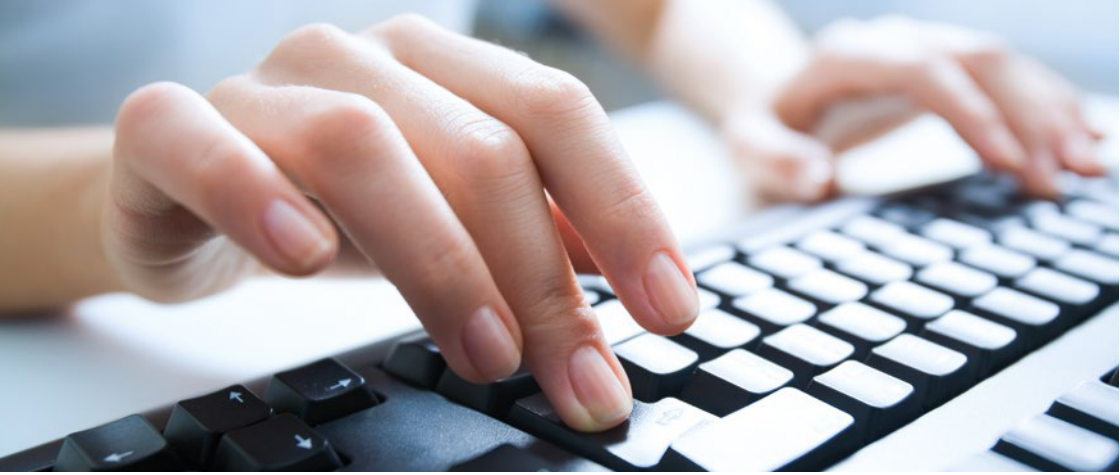
The GDPR strengthens individuals' data rights and creates new rights which charities will need to familiarise themselves with and act on, such as the right to data portability, the right to erasure and the right to object to processing. Under the GDPR it will not be possible to charge a fee for responding to a subject access request and the timeframe for responding has been reduced (without delay and no later than one month of receipt).

Processors

The GDPR introduces direct, statutory data protection obligations on data processors. Under the DPA, processors are generally not subject to direct obligations, fines or other penalties and so this represents a significant change.

4. What are the risks of breaching the GDPR?

Under the DPA the maximum fine that can be imposed for a data protection breach in the UK is £500,000. The GDPR significantly



increases this. Under the GDPR the ICO can impose a fine of up to 4% of annual worldwide turnover for the preceding financial year or EUR20 million (whichever is greater) for certain data protection breaches.

Furthermore, charities will have to report "notifiable breaches" to the relevant supervisory authority (the Information Commissioner's Office in the UK) within 72 hours. In some cases the individual concerned must be notified as well.

5. Will the changes have any effect on personal data obtained prior to 25 May 2018?

Yes. The GDPR will apply to all personal data held by a charity irrespective of when that data was obtained. Charities should therefore be looking now at what personal data they process and on what lawful basis that data is processed (and whether it will still be considered lawful on 25 May 2018). For example, if a charity processes personal data based on the individual's consent, but the consent obtained from the individual does not meet the higher standards imposed by the GDPR, the consent will not be valid once the GDPR comes into force. In such circumstances the charity should obtain fresh consent from the individual which meets the requirements of the GDPR before 25 May 2018 to ensure that it can process that individual's personal data lawfully once the GDPR comes into force.

Similarly, whenever a charity shares personal data with a third party data processor, it should have an appropriate data processing agreement in place with that processor. The GDPR stipulates the provisions which have to be included in a data processing agreement and they are more extensive than under the DPA. Any arrangements charities have in place with third parties where they are sharing personal data should be reviewed and, where necessary, updated prior to 25 May 2018 to ensure compliance with the GDPR.

6. Will there be any transitional 'bedding in' period within which to achieve compliance?

No – compliance will be required from 25 May 2018. It is therefore important that charities (if they have not done so already) ensure that they review their existing policies and procedures to ensure they comply with the new laws and make any necessary updates – such as to methods of obtaining consent. Staff should be trained and educated in the new laws and any related changes to the charity's existing procedures.

If you have any queries on any issues raised in this document please contact David White on 01482 337209 or email david.white@rollits.com

Hull Office
Citadel House, 58 High Street, Hull HU1 1QE
Tel +44 (0)1482 323239

York Office
Forsyth House, Alpha Court, Monks Cross, York YO32 9WN
Tel +44 (0)1904 625790

rollits.com

Authorised and Regulated by the Solicitors Regulation Authority under number 524629
Rollits is a trading name of Rollits LLP. Rollits LLP is a limited liability partnership, registered in England and Wales, registered number OC 348965, registered office Citadel House, 58 High Street, Hull HU1 1QE.
A list of members' names is available for inspection at our offices. We use the term 'partner' to denote members of Rollits LLP.
November 2017