Crowe

General Data Protection Regulation

What your charity should be doing now to prepare for May 2018

Audit / Tax / Advisory / Risk

Smart decisions. Lasting value.

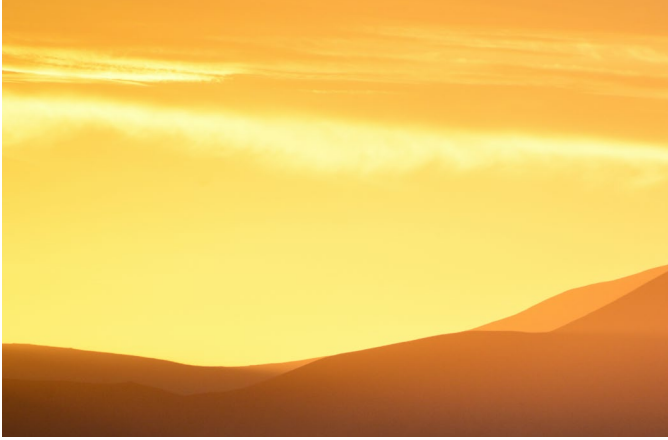
In this issue

On 25 May 2018 the General Data Protection Regulation (GDPR) will replace the Data Protection Act 1998 (DPA). This will change the way you collect, store and process personal data.

The GDPR has been adopted by the European Commission and will have implications for all organisations which control and process personal data. The impact of this change is extensive and wide-ranging, in particular for organisations within the charity sector.

The GDPR applies to all 'data controllers' and 'data processors'; terms that are defined broadly in line with the DPA.

The landscape of post-Brexit GDPR is uncertain, but the UK government has already confirmed the GDPR will apply in the UK.



Is this relevant for my charity?

The GDPR, like the DPA, will apply to all 'personal data'. It is therefore almost certainly relevant to you. Personal data under the GDPR is defined as:

"any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person".

The GDPR extends the former DPA definition to include 'location data', 'online identifiers' and 'genetic data'. This will bring new data sets within the scope of the regulation, for example IP addresses.

Most charitable organisations hold vast amounts of personal data (from HR details for staff to donor databases).

The definition of 'sensitive personal data', a term familiar from the DPA, remains broadly unchanged.

The new legislation applies to all data controllers[1] and all data processors[2], with the definitions remaining broadly unchanged from the DPA. If your charity previously fell within the scope of the DPA, then almost certainly the new GDPR will apply to you.

Much has been made of the widened territorial scope of the GDPR. The new legislation applies to organisations who process personal data about EU subjects, irrespective of where the actual data processing takes place.

[1] Data Controllers: A person or body, alone or jointly, which determines the purpose and means of processing personal data.

[2] Data Processors: An entity which processes the data on behalf of a data controller.

Key principles of the GDPR

The GDPR sets out responsibilities under a set of principles:

- fairness
- lawfulness and transparency
- purpose limitation
- data minimisation
- data quality
- security
- integrity and confidentiality.

One of the most significant changes from the DPA is the principle of accountability which requires your organisation to show how it complies with the principles.

Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) of the GDPR requires that:

- The controller shall be responsible for, and able to demonstrate, compliance with the principles.

Most notable changes from the DPA

The key changes in the GDPR are:

- stricter criteria for consent
- additional details specifically in reference to children's consent
- the accountability concept
- "the right to be forgotten"
- other enhanced rights
- cross border transfers.

Consent

The conditions within the GDPR include:

- the data subject must have the right to withdraw consent at any time, and it must be as easy to withdraw as it is to give
- consent mechanisms will need to be genuine and granular – 'catch-all' consents will likely be invalid
- the individuals must take affirmative action to provide their consent, such as signing a form or ticking a box
- consent must be freely given, informed and specific.

Transparency

Organisations must give data subjects extensive detail about how their data will be processed.

Data Controllers are required to present this information in a concise, transparent, intelligible and easily accessible way. The information that must be provided includes details about the rights of the data subject, for example the right to withdraw consent, and must be given at the point of collecting the data.

Children and consent

Children below the age of 13 can never give consent to the processing of their personal data in relation to online services. Some national flexibility is given for children between the ages of 13 and 15. Those aged 16 or older may give consent for the processing of their personal data themselves.

Regulated data

The GDPR highlights a number of online identifiers, such as cookie IDs and IP addresses, which may be personal.

Data Processors

Under the GDPR, data processors have direct obligations. These include maintaining a written record of processing, and notifying the controller of any personal data breaches without undue delay.

Accountability

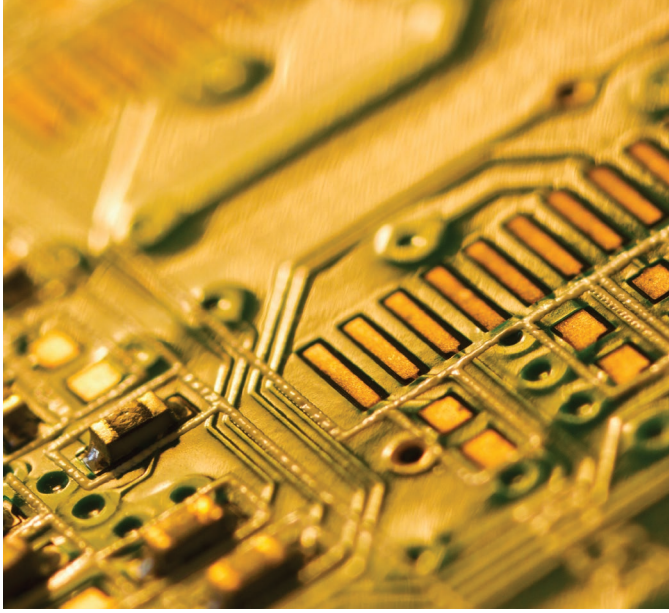
One of the key changes is the onerous accountability obligations placed on data controllers to demonstrate compliance. This includes keeping documentation of decision making to evidence active compliance with the GDPR.

In certain circumstances organisations must name a Data Protection Officer (DPO), the DPO is required to have sufficient expertise to carry out this role.

Enhanced rights for individuals

Reinforcement of the rights of the individual is a clear aim of the new legislation. The GDPR enhances rights of individuals in a number of ways including:

- access rights to the data being processed about them (in certain circumstances)
- correction rights where data is wrong
- the right to restrict certain processing
- the right to object to personal data being processed for direct marketing
- the right to data portability
- the right to be forgotten/the right to erasure.



Requests from data subjects to exercise these rights must be responded to within one month. This is a shorter time limit than the 40 days allowed under the DPA.

Reporting requirements

GDPR requires mandatory notification of any breach to the relevant Data Protection Authority: the Information Commissioner in the UK. Notification needs to be made without undue delay, and where possible, within 72 hours of the breach.

Cross border data transfers

The international transfer rules remain substantially unchanged. The legitimate basis for transferring personal data needs to be considered, as does the protection of that data once overseas.

Why is this a priority for my organisation?

Most charitable organisations hold vast amounts of personal data, such as names and addresses of donors, supporters, and beneficiaries. Many also hold sensitive personal data such as racial or ethnicity details, information regarding religion, physical or mental health conditions, or criminal record details.

The charity sector has significant legal and moral obligations to protect this data from harm.

Compliance with the GDPR is a legal requirement from 25 May 2018. Non-compliance could lead to substantial fines.

The GDPR sets two tiers of fines, with no provision or exception for organisations which are 'for the public benefit'.

The top tier fine is up to the higher of 4% of annual worldwide turnover and EUR20 million. Other specified breaches would incur a fine of up to the higher of 2% of annual worldwide turnover and EUR10million. The level of the fine will reflect the nature, gravity and duration of the breach.

In addition to a fine, non-compliance risks substantial reputational damage.

Individuals demand protection of their personal information. Charitable organisations need to consider the potential damage to reputation of any breach. To minimise reputational risk, many organisations extend data protection controls well beyond the scope of legal requirements.

Prepare now for GDPR in May 2018

The principles of the new GDPR legislation are familiar from the DPA, but the obligations in some areas are more extensive. Charities need to ensure their internal processes and IT systems will be able to cope with the new regulation from May 2018.

Steps your charity should take:

- assign responsibility and budget for data protection compliance within your charity
- consider assigning responsibilities to a 'Data Protection Officer' – even where there is no legal requirement to do so in the GDPR
- run a compliance gap audit, to address possible areas of non-compliance
- audit the legal basis on which you currently collect and process personal data:
  - review what data you currently collect
  - check what consent you obtain: is this sufficient to meet the new GDPR requirements?
  - check privacy notices are clearly worded and easily accessible
- update risk registers, and use risk management tools to tailor your response to the results of the compliance gap audit
- consider updating job descriptions and job specifications for data protection responsibilities
- put in place policies and procedures to ensure data breaches are identified and dealt with promptly, including an agreed chain of communication to relevant authorities
- develop template responses, to ensure communications are GDPR compliant

- establish a framework for accountability, to prove your organisation meets the required standards for data protection under the GDPR
- ensure your staff are adequately trained and understand the new obligations
- audit the systems and controls surrounding any high risk data processing, to ensure appropriate steps are taken to address any specific weaknesses or concerns
- ensure data protection and privacy is embedded into all decision making, and forms part of all strategic discussions
- consider the 'right to erasure' – will your systems be able to comply with requests of this nature?
- consider whether the consent rules for children are likely to affect your organisation
- consider your relationships with your data processors (outsourced payroll providers for example) and ensure lines of responsibility for data protection are clearly defined in service agreements
- review, map and audit any international data transfers and consider:
  - are they necessary
  - do you have a legitimate basis for transferring the personal data
  - how is the data protected once overseas?
- consider developing data subject access portals to pass administration of the data directly to the individuals
- review marketing suppression lists and other marketing procedures to ensure they are GDPR compliant
- discuss and consider reputational risk above and beyond the requirements of GDPR.

How Crowe can support you

Working with Crowe gives you access to a team of specialists, who can:

- map your current systems and controls operating to protect your data
- review procedures in place within your organisation
- assess the design and effectiveness of your key controls
- identify weakness in your systems and put forward recommendations
- help your team prioritise actions into urgent, important and non-essential
- raise the profile of compliance within the operational team.

If your organisation predominantly holds data electronically and relies heavily on your IT infrastructure and web based systems, Crowe can also support you and your organisation to:

- identify strengths, weaknesses and potential gaps in IT controls based on internal and external threats
- identify where controls could be developed
- compare your system and procedures against best practice for:
  - network security (including firewall and network setup, vulnerability testing, remote access, and email security)
  - computer security (covering anti-virus, patching and removable devices)
  - user access security (covering user management, administrators, passwords and physical access)
  - ICT Management and User Awareness (covering policies and procedures, user training, third party management and incident response)
  - data management (covering data ownership, data protection, and data processing)
  - change management procedures
  - disaster recovery procedures.

Start the conversation

Guy Biggin
Partner
guy.biggin@crowe.co.uk
+44 (0)1242 234421

About Us

Crowe UK is a national audit, tax, advisory and risk firm with global reach and local expertise. We are an independent member of Crowe Global, the eighth largest accounting network in the world. With exceptional knowledge of the business environment, our professionals share one commitment, to deliver excellence.

www.crowe.co.uk

@CroweUK

Crowe U.K. LLP is a member of Crowe Global, a Swiss verein. Each member firm of Crowe Global is a separate and independent legal entity. Crowe U.K. LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Global or any other member of Crowe Global.

© 2018 Crowe U.K. LLP