BRODIES LLP

WHAT DOES THE GDPR MEAN FOR...**CHARITIES?**

The General Data Protection Regulation comes into effect on 25 May 2018 and will introduce a number of substantive changes to data protection laws across Europe. The changes are likely to be supplemented by new rules in relation to electronic marketing and online tracking.

The GDPR will require all organisations to review how they collect, hold and process personal information and how they communicate with individuals. Organisations will need to adopt new measures and update their internal processes to demonstrate their compliance with the GDPR. The new rules will be backed up by enhanced enforcement powers.

Changes include:

Consent
There is a new requirement for 'clear affirmative action' and an end to pre-ticked boxes and bundled consents.

Transparency
Organisations must provide much more information to individuals.

Lawful Processing
There are stricter rules on processing data for new purposes.

New access rights
Greater rights are given to individuals, including rights of erasure, protection against profiling, and a right of data portability.

Privacy by design and default
Existing good practice recommendations must be hard-wired into day to day operations.

Breach notifications
New express obligations to notify privacy regulators and affected individuals in the event of certain data privacy breaches.

Accountability
Organisations will have to demonstrate compliance to regulators on an ongoing basis and maintain records.

Sanctions
The power for regulators to issue fines for up to €20m or 4% of worldwide turnover, (including substantial fines for administrative breaches).

We always get excellent service from them. They always understand what we're looking for, they communicate in plain English, stick to timelines and always deliver.

Data Protection & Information Law, Chambers & Partners 2016

How will this affect me?

Charities process large amounts of personal data – not just in relation to donors, but also employees and volunteers, and also any service users. That information may be held on systems within a charity or processed by third parties, for example outsourced service providers or fundraising partners. Depending on the particular functions of the charity, the information held may include special categories of personal data, such as medical information, which are subject to stricter rules.

Many charities work together with other third-sector organisations, or public bodies, in order to provide their services. GDPR will change the rules on how these relationships are governed, and how risks and responsibilities are apportioned between parties.

The Information Commissioner has recently taken enforcement action against a number of charities in relation to the misuse of data in connection with fundraising activities. Charities should ensure that their fundraising activities are compliant with data protection and electronic marketing laws, including new rules on consent.

Specific issues:

- **Data collection** - do your privacy notices and processes for collecting personal information meet the new rules on transparency and consent?
- **Fundraising/marketing consent** - do you obtain appropriate consent to send individuals electronic marketing? Are your existing consents acceptable?
- **Marketing lists** - if you acquire marketing/fundraising data from third parties, are you confident that you have the right to use that information?
- **Policies and processes** - have you reviewed your data policies and processes for allowing individuals to opt out of future marketing? Do you use email or online tracking or profiling?
- **Partnership working** – do you have a clear understanding of the nature of each partnership? Do you know what your role and responsibilities are in relation to handling of personal information?
- **Data security** – are your staff and volunteers provided with the tools to keep data secure?
- **Data retention** - how long do you retain information? Do you have a data cleansing policy?
- **Third party agencies** - if you use third parties to process personal information, have you reviewed your contracts with them to ensure that they contain appropriate controls on the use of your data?
- **Data sharing** - if personal information is shared with third parties, is that being done on a fair, lawful and transparent basis and is the information sharing underpinned by an appropriate written contract?

What do I need to be doing?

- Identify **your team** and **plan your strategy** for compliance.
- Create an **information asset register** – what personal information and where, why, how and with whom do you process it.
- Review the **legal basis** for your data processing activities, particularly fundraising.
- Review your **data collection forms** and **privacy notices** to ensure they meet the new requirements.
- Review your **processes and systems** for dealing with data subjects rights.
- Implement **data governance** policies and measures and **training** to ensure your organisation operates in accordance with the requirements of the GDPR.
- Review your **arrangements with data processors** and other third parties.
- Ensure that new technology and systems are **GDPR ready**.

Key contacts

To discuss how the GDPR will impact on your organisation, or how Brodies can assist you with your preparations, please get in touch with a member of Brodies' data protection and information law team.

Grant Campbell
PARTNER
+44 (0)131 656 0115
grant.campbell@brodies.com

Martin Sloan
PARTNER
+44 (0)131 656 0132
martin.sloan@brodies.com

Alan Eccles
PARTNER
+44 (0)141 245 6255
alan.eccles@brodies.com

Follow the latest developments on the GDPR, including our latest blogs and guidance from regulators, on our GDPR microsite: **brodies.com/GDPR**