BRODIES LLP

WHAT DOES THE GDPR MEAN FOR...**PROFESSIONAL SERVICES?**

The General Data Protection Regulation comes into effect in mid-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?

Professional services firms will handle personal data in various situations. They will hold personal data relating to employees and, possibly, contractors. They will also hold personal data relating to clients and potential clients in CRM systems, case files and marketing databases. Finally, firms may also hold personal data relating to contractors and other third parties with whom they engage from time to time on projects.

In most cases, the ICO's view is that professional services firms such as law firms and accountants will be data controllers when providing services to their clients. However, there may be certain situations where a professional services firm acts as a data processor on behalf of another organisation. This distinction is important and will require analysis on a case by case basis.

Specific issues:

- **Data collection** - do your privacy notices, client engagement and processes for collecting personal information meet the new rules on transparency and consent?
- **Legal basis for processing** – have you identified the basis upon which you process personal data?
- **Marketing consent** - do you obtain appropriate consent to send individuals electronic marketing?
- **Policies and processes** - have you reviewed your data policies and processes for handling subject access requests and other data subject rights?
- **Data retention** - how long do you retain information on your systems? Do you have a data cleansing policy? How does that fit with your regulatory obligations?
- **Contracts** – if you use third parties to handle personal data on your behalf (for example providers of IT systems or marketing agencies), do your contracts comply with the requirements of GDPR?
- **Workforce data** - what information do you hold? How long do you retain it for? Do you need to hold that information? Do you monitor staff? Is the processing fair and lawful?
- **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?
- **Breach reporting** – do you have internal processes in place to deal with data breaches and ensure that they are reported to the ICO? Do your staff know what to do if they suspect a data breach has occurred?

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.
- 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, including new rights in relation to erasure of data and data portability and your use of profiling.
- Implement **data governance** policies and measures and **training** to ensure your organisation operates in accordance with the requirements of the GDPR.
- Review your **supply chain arrangements** with data processors.
- Ensure that new technology and systems are **GDPR ready**.

More information

You can follow the latest developments on the GDPR, including the latest guidance from regulators, on our GDPR microsite:

brodies.com/GDPR

or our blog:

http://techblog.brodies.com

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

Christine O'Neill
PARTNER
+44 (0)131 656 0286
christine.oneill@brodies.com

Charles Livingstone
PARTNER
+44 (0)131 656 0273
charles.livingstone@brodies.com