The General Data Protection Regulation

The General Data Protection Regulation (GDPR) will come into force on 25 May 2018 and will usher in a tougher new EU-wide data protection regime that will have direct effect in member states. Despite Brexit, the UK Government has confirmed that GDPR will come into force in the UK in May 2018 as originally planned.

The GDPR represents the most fundamental shake-up of data protection law in over 20 years. The GDPR will require all organisations to review how they collect, hold and process personal information and how they communicate with data subjects. Organisations will need to adopt new measures and principles into their internal processes to demonstrate their compliance with the GDPR. The new rules will be backed up by enhanced enforcement powers.

Changes introduced by the GDPR include:

Consent - the requirements for 'consent' are tightened so that 'clear affirmative action' will be required for consent to be established. The days of pre-ticked boxes will finally come to an end.

Transparency - organisations must provide more information to individuals at the point of collection to explain in more detail how that data will be used, how long it will be retained and, if it to be stored outside the EEA, where it is to be held and how it is to be safeguarded.

Lawful Processing - new rules on processing for new purposes. Public sector organisations will no longer be able to rely on the 'legitimate interests' condition.

Access - the rules allowing individuals to access their personal data and to obtain information about how that data is being used are being strengthened and the timescale for responding is being shortened. New rights will enable a right of erasure and a right for data portability.

Privacy by design and default - organisations will be obliged to 'hardwire' privacy considerations into their day-to-day operations and projects through measures such as minimising the amount of data held and activating privacy-friendly settings in technology.

Breach notifications - there are express statutory obligations to notify privacy regulators and affected individuals in the event of a data privacy breach where there is risk of harm to individuals.

Accountability - organisations will have to be able to demonstrate to privacy regulators that they are complying with the GDPR on an ongoing basis.

Sanctions - the maximum fines that can be imposed for serious contraventions are €20m (or 4% of total worldwide turnover for businesses) but lesser contraventions also carry hefty fines.

As a Regulation, the GDPR will have direct effect in EU member states without the need for any national implementing legislation. The intention is to ensure that there is no scope for member states to water down the key principles of the GDPR and regulators in each state will be expected to toe the line through 'consistency' mechanisms, which may curtail the UK regulator's current light touch regime.

Now that the UK Government has removed any lingering uncertainty that the GDPR might not come into force in the UK as a result of the Brexit process, organisations that have not already begun preparing for the GDPR need to start planning now. Failure to comply may expose the organisation to significant legal compliance risks and penalties but, with individuals becoming increasingly concerned about how their data is handled and protected, those who do not take GDPR seriously risk losing the trust of the individuals whose data they handle as well as significant reputational damage. In some cases, the consequences may be existential.

Preparing for change

Organisations need to invest heavily in systems and resource to ensure that they will be compliant by May 2018. We can help you prepare for GDPR by providing you with step-by-step legal guidance that understands both GDPR and the associated regulatory guidance, as well as emerging market practice and norms, helping you to carry through your GDPR project efficiently and with the minimum of disruption.

Follow the latest developments on the GDPR on our hub:

brodies.com/GDPR

Brodies has provided us with a high level of service, with prompt response times and concise advice. They are excellent. Always our first port of call in Scotland.

Chambers and Partners 2017 - Data Protection and Information Law

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.

Key contacts

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