Linklaters

The General Data Protection Regulation – December 2015

In force 2018

Political agreement on the GDPR was reached on 15 December 2015. It should be formally adopted in 2016 and come into force in 2018. The agreed text is here.

Expanded scope

The GDPR will apply to data controllers established in the EU and also to:

- businesses outside the EU that deal with EU citizens; and
- data processors.

Core rules remain the same

Many of the core principles are similar to those in the 1995 Data Protection Directive. However, there are some significant amendments to these principles and significant new obligations.

What are the sanctions?

The sanctions for breach of the GDPR are significant. Regulators can impose fines of up to:

- 4% of total annual worldwide turnover; or
- €20,000,000.

Are there new data security rules?

Yes. Data controllers must notify regulators of data breaches within 72 hours, unless the breach is unlikely to be a risk to individuals. If there is a high risk to individuals, those individuals must be informed as well.

There are also new data security requirements including:

- additional obligations for contracts with data processors; and
- provisions that recommend the use of encryption, back up and pen testing.

Accountability

Under the GDPR, controllers must not only comply but be able to demonstrate they comply, e.g. through the use of policies. Controllers must carry out privacy impact assessments for "high risk" processing.

Can children give consent?

Children under 16 need parental approval to consent to the processing of their personal data online. Member States can reduce this minimum age to 13.

What should I do now?

The GDPR will not come into force until 2018. However, there is a lot of work to do in the meantime. You should:

- determine if you are newly caught by these rules, e.g. if you have direct liability as a data processor;
- review customer-facing materials to comply with new consent and transparency requirements;
- review and amend contracts with data processors; and
- consider setting up a central breach management unit to report breaches.

You also need to review the compliance of all your processes, not only as part of your "accountability" obligations but also to mitigate risk under the new sanction regime.

Will it be harder to get consent?

Yes. Consent must be "unambiguous" (or "explicit" in the case of sensitive personal data or transborder dataflow). A written request for consent must be separate to other written materials.

Do I have to appoint a DPO?

Organisations that are involved in the systematic monitoring of individuals on a large scale or who process large amounts of sensitive personal data must appoint a data protection officer.

What about cross-border dataflow?

The rules on transferring personal data out of the EU are broadly similar, though slightly more restrictive, particularly where the transfer is part of litigation or for a regulatory investigation.

Do individuals have new rights?

Yes. Individuals have the right to be "forgotten", the right to data portability and the right to object to profiling. These are complex rights. It is not yet clear how they will operate in practice.