



WHAT DOES THE GDPR MEAN FOR...TECH START-UPS?

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 at the point of collection.



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

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 demonstrate compliance to regulators on an ongoing basis and maintain records.



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.



One stop shop

There will be a simplified regulatory oversight for organisations that operate in multiple countries in the EU.



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.



How will this affect me?

Many technology start-ups are data-driven businesses. The GDPR will require technology businesses to review how they use and handle personal data.

For start-ups, it's important to be able to show that the business has been designed to be GDPR-ready, as compliance issues may cause an issue when seeking investment or an exit. Indeed, there may be a competitive advantage in embracing the GDPR and showing that protecting the privacy of users is part of the business's DNA.

Specific issues:

- **Privacy notices** - you will need to provide much more information – particularly in the relation to profiling and analytics
- **Lawful basis** - you'll need to ensure that you have identified a lawful basis for your processing. If you rely on consent, then it must be specific, informed and unambiguous
- **Children** - where online services are used by children, you'll need a system to obtain parental consent and carry out age verification
- **Cookies and tracking** - the rules on using tracking technologies in apps and on the web will likely be updated, which may require you to adopt new ways for controlling preferences
- **Privacy by design** - your systems will need to be built using the principles of privacy by design, using privacy impact assessments to identify risks
- **Data subject rights** - you'll need to design your systems to enable individuals to easily exercise their rights, including their right to erasure and right to move their data to another service provider
- **Data minimisation** - when using big data and data analytics, you'll need to consider data minimisation and anonymisation
- **Data protection officer** - depending on the type of data you collect, you may need to appoint a DPO
- **System monitoring** - you'll need to have processes to deal with monitoring and reporting cyber-attacks and other security breaches within the required timescales



What do I need to be doing?

- Identify your team and **plan your strategy** for compliance
- Create an **information asset register** – who, what, where and with whom do you share personal information?
- Review the **legal basis** for your data processing activities
- Review your **privacy notices** to ensure they meet the new requirements
- Review your **processes and systems** for dealing with data subjects rights
- Implement appropriate **data governance** policies and training
- Review your **supply chain arrangements** with data processors (including your cloud hosting provider)
- 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

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