Cooley

December 18, 2015

After nearly four years of waiting and constantly moving deadlines, the European Parliament has finally agreed the text of the new General Data Protection Regulation (GDPR).

What's the big deal?

It has been 25 years since the last overhaul of data protection law in Europe and considering how far the Internet, and technology generally, has come during that time, the update is well overdue. Previously, EU Member States had leeway to construct their own data privacy rules, which hindered harmonisation and made it difficult for companies operating globally to understand and ensure compliance. The new regulation is intended to remove this incoherency and is directly applicable in all 28 Member States.

With the landmark ruling last year on "the right to be forgotten" and the recent invalidity of the US-EU Safe Harbor scheme in October, the global privacy landscape looks to be changing for fast and companies and organisations of all shapes and sizes need to get up to speed. Andrus Ansip, Vice-President for the Digital Single Market called the agreement a major step towards a Digital Single Market, removing barriers and unlocking opportunities, with the highest data protection standards.

So what's new?

The good

- There will only be one set of rules, making it simpler and cheaper for companies to comply and quite frankly, do business in the EU.
- Businesses will deal with one single supervisory authority (rather than multiple regulators in the various jurisdictions), which is estimated to save €2.3 billion per year.
- Innovation is also one of the key aims, with the regulation guaranteeing that data protection safeguards are built into products and services from the earliest stage of development.
- Privacy-friendly techniques such as pseudonomysation will also be encouraged to reap the benefits of the innovative field of big data whilst ensuring the rights of the individual are protected and respected.

The bad

- Companies and organisations will be required to appoint data protection officers and to obtain express consent from users for access to personal data.
- Once a purpose for collecting and using data is stated, that's it: the data cannot be used for any other purpose.
- Companies will also be required to publicly declare serious data breaches within 72 hours and notify individuals if the breach is likely to result in a high risk to their rights and freedoms to allow them to take the necessary precautions.

The ugly?

- Increased sanctions: companies that fail to abide by the new rules could be fined up to 4% of their worldwide annual turnover. This could mean fines totalling billions for the bigger fish in the sea, although it has not yet been confirmed whether this will apply to the controlling undertaking or be confined to the entity in breach.

What about SMEs?

The reform aims to help SMEs break into new markets and cut costs and red tape by abolishing notifications to supervisory authorities and allowing SMEs to charge for data access requests that are manifestly unfounded or excessive. SMEs will also be exempt from the obligation to appoint a data protection officer as long as data processing is not their "core business activity" and will have no obligation to carry out an impact assessment unless there is a high risk.

How does this affect non-EU companies?

Just as the Internet does not respect international boundaries, the new rules will apply to companies who touch personal data of European citizens even if that company isn't based in the EU, presenting quite some challenge. It is very possible that different approaches to privacy around the world will only get more complex. Non-EU companies with access to personal data of EU citizens will need to pay close attention not only to what the EU is doing, but also how other countries' react to the EU's changes.

And US companies in particular?

US technology groups are not happy and up until the eleventh hour, lobbyists were fighting to dilute the restriction on companies handling data from under-16s without parental consent: a compromise was eventually reached allowing Member States to determine in their discretion the minimum age between the years of 13 and 15. Most US companies to whom this will apply will likely already comply with The Children's Online Privacy Protection Act (COPPA) restricting the minimum age to 13. If not, it might be worth following this line in the short term. The new legislation does not change the existing restrictions on data transfer outside the EEA; however, remember to keep an eye on the US-EU Safe Harbor 2.0 negotiations, which are yet to be finalised.

What now?

There is no need to panic just yet: the text needs to be officially adopted and the law will not be fully applicable for another two years. However, it is important not to underestimate what a step up the GDPR is from its predecessor Directive (and implementing legislation in the various Member States) and the groundwork that lies ahead.

Five practical steps

1. Check your current state of compliance with the existing EU Data Protection law by reviewing privacy and cookie policies, applicable agreements, correspondence and other data protection statements – if you are not complying or cannot comply with the existing regime, you will struggle with the GDPR;
2. Prepare a data incident response plan;
3. Improve data security by limiting access to personal data;
4. Provide internal training on data protection; and
5. Consider cyber insurance.

Please contact Sarah Pearce or another member of Cooley's London Privacy & Data Protection team, led by partners Ann Bevitt,

Mark Deem and Sarah Pearce who can help review your practices from an EU perspective and discuss your options going forward. They offer multi-disciplinary depth and breadth of experience to clients in data protection, privacy by design, data breach management, incident response, breach preparedness, and related litigation, especially in large breaches and those with multi-national issues.