GDPR - 6 months on

Cast your mind back to Spring this year and you may recall that barely a day went by, or so it seemed, without an email with an updated privacy notice or requesting your 'informed consent' landing in your inbox. GDPR was the topic that everyone was talking about - from the watercooler to the boardroom. It is 6 months since the regulation came into force and we consider whether the impact has matched the hype.

Did everyone meet the deadline for compliance?

Across all industries it was clear that the work required to comply with the GDPR was significant. Whether yours was a large multinational company with resources to dedicate, or a small local business trying to interpret the new legislation with little assistance, the pressure to ensure compliance was felt at all levels. Whilst some larger companies created entire new teams to ensure their business was compliant before the deadline, the sheer magnitude of what was required was beyond some businesses to achieve by 25 May 2018 or at all.

The IAPP-EY Annual Privacy Governance Report 2018 reported that fewer than 50 percent of those surveyed were "fully compliant", and nearly one in five admitted they considered that full GDPR compliance was "impossible" at any time. Whether it is enough to have 'done all you can' within the limitations of your business will depend on how the Information Commissioner's Officer ("ICO") interpret any breaches that occur.

James Dipple-Johnstone, the ICO's Deputy Commissioner (Operations), has said that companies that make the right commitments to customers will have little to fear from an ICO inspection or investigation.

Although this guidance should not be interpreted as an excuse to overlook areas of non-compliance, the ICO will not take issue where companies can show they have taken their responsibilities under the GDPR seriously.

What complaints / notifications have been made under the new regulation?

As expected, since May 20108, the ICO has been inundated with complaints and notification breaches. (Within hours of the GDPR coming into force, the first complaints were filed against Facebook and Google.) Data requested from the ICO by the law firm, EMW, showed that complaints had risen by 160 percent in the 6-week period following 25 May 2018 compared with the same period the previous year.

Speaking at the CBI Cyber Security Conference, Dipple-Johnstone reminded businesses that they need to devote sufficient resources to dealing with data breaches. He noted that there was a tendency towards overly cautious reporting which meant that a large percentage of the significant number of calls received by the ICO resulted in the organisation ultimately deciding that the breach did not meet the reporting threshold. Although this was to be expected at first, the ICO has confirmed that they will start to discourage this practice and will expect business to be familiar with the reporting threshold.

Enforcement and fines

Although the potentially huge penalties were a significant point of discussion, since its implementation, only a handful of companies have been sanctioned under the new rules and the penalties have been unremarkable.

The most notable in the UK is AggregateIQ, a Canadian analytics firm which worked for the 'Vote Leave' campaign, and became the first company to receive a formal notice under the GDPR (which it is currently appealing). A German chat platform received a fine of €20,000 for incorrectly storing user passwords, a retailer in Austria was fined €4,800 for installing CCTV which recorded images from a public pavement and a Portuguese hospital received a €400,000 fine for violations relating to access to patient data (also under appeal).

It is possible that the penalties have been relatively small so far because the more significant breaches are still being investigated. We know that the ICO is currently investigating British Airways for its security breach earlier in the year and there are likely to be consequences for Facebook following the breach which affected 50 million accounts worldwide.

Giovanni Buttarelli, the European data protection supervisor, told Reuters in an interview in October 2018 that he expects more fines to be announced by the end of the year, which means we may start to see more significant penalties emerging over the coming months.

Impact on the US

The GDPR applies to all companies processing and holding personal data of EU residents, regardless of the company's location. However, the international impact has been less than expected. In the US, California has implemented what has been referred to "GDPR lite" which comes into force in 2010 and Oregon is trying to introduce a Privacy Law Bill, though it is doubtful whether it will succeed.

Many US businesses have largely ignored the GDPR. Some (for example, the LA Times and the Chicago Tribune) have made their publications inaccessible to those based in the EU, taking the view that they would rather lose those international readers than invest time and money ensuring compliance.

It may be that the US is watching and waiting for the significant penalties to be handed out before determining the level to which they need to need to 'toe the line'.

CPB Comment

Whether or not the GDPR has made the impact expected within its first 6 months, one thing is certain: data protection awareness has come to the forefront. Individuals are aware of their rights and are more willing to enforce them. As a result, companies are being held accountable for failing to protect those rights. In a progressively more digital age, where almost unfathomable amounts of personal information can be transported globally at the click of a button, any increase in awareness of how to protect against an abuse of that power must be considered a step in the right direction.

One last thing

It is easy for business to think that now the GDPR is in force, and the initial flurry of activity has subsided, there is currently little that needs to be done. However, GDPR compliance is an on-going issue and checks and balances that were put in place before May 2018 may already be out of date. It is good practice to continually review your data protection policies and procedures, not only to ensure that they remain adequate but to ensure they are being enforced across the business. Keeping data protection as a regular topic, from the office training manual to the boardroom, is a key way to ensure your company is protected against potential complaints to the ICO or being required to report your own data breaches. There is no time like the present – now is an opportune moment to undertake the first of your GDPR evaluations!

Samantha Zaozirny
Associate

T: 0203 697 1906
M: 07780221676
E: samantha.zaozirny@cpblaw.com