GDPR five months on: what we've seen so far

By Peter Erceg

Despite recent data breaches, possible fines and compensation claims, companies should not just focus on compliance.

Most doomsday predictions made in the build-up to the General Data Protection Regulation's (GDPR) implementation have not come to pass. The last five months have, however, given companies much to think about.

High-profile social media companies Facebook, WhatsApp and Instagram, as well as search engine Google, were all hit with complaints to regulators within hours of GDPR becoming effective on 25 May. Investigations into each are thought to be ongoing.

The UK Information Commissioner's Office (ICO) received 657 notifications in May and 1,752 notifications in June, compared with its previous average of around 350 notifications per month.

The ICO's first ever violation notice of GDPR was issued in July against AggregateIQ, a Canadian data analytics firm linked to the Facebook-Cambridge Analytica scandal.

The ICO notice accuses AggregateIQ of violating GDPR rules because it "processed personal data in a way that the data subjects were not aware of, for purposes that they would not have expected, and without a lawful basis for that processing".

The firm gathered all the data under question before 25 May 2018, but it was still holding the data when the law came into effect, making it liable, the ICO said. And while the company is not an EU entity, the ICO ascertained that it is still subject to GDPR because AIQ processed personal data of data subjects within the EU.

This will certainly not be the last notice sent as part of the GDPR regime. Perhaps the most significant incident to date (at least in terms of its possible implications for other UK-based companies) has been the British Airways (BA) data breach.

Size of fines

On 7 September BA announced that nearly 400,000 customers' personal and financial data was compromised. It is one of the UK's largest data breaches – and one of the first documented large-scale breaches to occur in the UK since GDPR became effective.

The data breach could set a strong precedent in two respects:
1) the size of fines that the ICO issues for breaches of GDPR, and
2) the outcome of possible class actions.

Under GDPR, fines imposed following a data breach can be up to 4% of the company's annual global revenue or £17 million, whichever is greater. In BA's case, a possible 2% fine (in light of the breach's nature) could amount to approximately £250m, based on BA's published annual reports for 2017.

> "Companies might also be liable for compensating customers for 'non-material' damage.

It is unlikely that BA would be penalised with such a large fine, because of how the Regulation is applied and the measures adopted by BA. Having said that, the ICO has traditionally taken a dim view of companies that haven't got the basics right. In the case of BA, it seems likely that a technique called cross-site scripting (or XSS) was used to inject malicious JavaScript code into their server or servers. XSS is a well-known vulnerability – it's actually number three on the Open Web Application Security Project's top-10 list of the most critical security risks.

Whatever the eventual size of any fine issued to BA, it could well indicate how the ICO will treat (and fine) other companies that are breached.

'Non-material' damage

Under Article 82 of GDPR, any person who has suffered material or 'non-material' damage as a result of an infringement of the Regulation has the right to receive compensation for the damage suffered. This could include a claim for (but not limited to): distress; anxiety; reputational damage.

> "Companies with a presence in the US could be at risk of lawsuits for not managing the effect of GDPR on their financial performance.

SPG Law – the UK arm of US law giant Sanders Phillips Grossman – launched a £500m group action against BA hours after the breach was announced. The law firm said it has launched the group action following BA's failure to offer financial compensation to individuals affected by the data breach for the inconvenience, distress and misuse of their private information. SPG Law estimates that each affected person may be able to claim up to £1,250 in compensation against BA.

Courts have not yet released any judgment for such compensation claims brought under GDPR. However, it is possible that this liability could be significant for companies if they face claims from multiple claimants for a breach of data. It might validly be predicted that the significant cost of prosecution will be far outstripped by the cost of private claims, fuelled by the development of 'claims farming' and a much greater understanding by data subjects of their rights and remedies.

Management liability

Companies with a presence in the US and other parts of the world could be at risk of lawsuits for failing to manage the impact of GDPR on their financial performance.

Investors recently filed a lawsuit in the Southern District of New York against global data management firm Nielsen, its CEO and CFO – over claims it delivered misleading statements on GDPR readiness and the impact the regulation would have on its business.

The case is significant because shareholder claims do not allege violations of the GDPR, but are grounded in US securities law on the basis the defendants failed to prepare for the Regulation and made misleading representations that they had.

> "Business value can be lost if the focus is only on satisfying the regulatory requirements of GDPR.

It follows a securities suit in the US against Facebook itself in July. The company's quarterly earnings disappointed investors, in part because the company was affected by allegedly unanticipated expenses and difficulties in complying with the GDPR.

It is likely that Facebook and Nielsen won't be the only companies that experience financial effects from the impact of GDPR and other privacy regulations. Other companies might also experience disruption as their customers, vendors, suppliers and partners implement processes and procedures to ensure GDPR and other privacy-related compliance.

Compliance is not enough

Organisations must remember that GDPR is a substantial business risk as well as a compliance issue. It cannot be treated as an add-on and must be integrated into the business, particularly in any training it does.

Substantial business value can be lost if a company is focuses purely on satisfying the regulatory requirements of GDPR. Companies should also actively consider how it can help to preserve or even grow business value. For example, the wording of an opt-in consent notification – ie, what it offers a customer – may be critical to the number of subscribers that are maintained.

Good corporate privacy programmes will bring many benefits, the most obvious being the ability to demonstrate to stakeholders (customers, shareholders, funders, regulators, and employees), that personal data and privacy is both taken seriously and managed well in the organisation, making the business a more attractive proposition generally.

The level of awareness that customers have of their privacy rights is likely to increase, especially if a breach of those rights might give rise to compensation; this will be accompanied by a corresponding raising of expectations in respect of the levels of fairness and transparency adopted by business in the collection and use of personal data. All other things being equal, businesses that are the most fair and transparent should have an advantage over their competitors.

Ultimately GDPR compliance should not drive a company's data privacy strategy – but simply validate it.

For information relating to this article please contact Peter Erceg on:
e: peter.erceg@uk.lockton.com
t: +44 (0)20 7933 2608