KPMG

General Data Protection Regulation

Wednesday 7 March 2018

KPMG Board Leadership Centre

FTSE350 breakfast with David Cooke, Information Commissioner's Office

Our first KPMG Board Leadership Centre FTSE350 breakfast of 2018 was a discussion about General Data Protection Regulation (GDPR) with David Cooke, a Non-Executive Director at the Information Commissioner's Office (ICO). The breakfast exposed both the complexity of the subject and that, for many, GDPR is still very much work in progress. Nevertheless, the pragmatic approach proposed by the ICO (see below) was well received by those in attendance. Eight key points arising from the breakfast were:

Brexit

1. Brexit is unlikely to have a significant impact on GDPR – not least because the legislation will be effective from 25 May 2018, long before the exit process will be completed. Furthermore, Theresa May has indicated that she not only wants the UK to have adequate regulation in this space, but that she wants the UK to be a leader and remain a full voting member of the European Data Protection Board. Data protection is only going to get more prominent as the internet of things, data mining and the backlash against 'tech giants' become more mainstream.

Pragmatism

2. The potential penalties for breaching UK data protection regulation have increased dramatically from a maximum of £500k under the existing legislation to a maximum of 4% of global turnover under GDPR. Nevertheless, the IOC seeks to be a proportionate, risk-based and pragmatic regulator favouring education and engagement - with enforcement as a last resort. For context, the maximum fine under the current regulations has never been levied and in 2016/17 only sixteen fines were imposed.

3. One attendee noted that pragmatism could be applied at two levels. Large organisations – which clearly need high standards – might be given some leeway for not having everything in place throughout the whole organisation on day one. On the other hand, small local charities running members' mailing lists might be carved out of the legislation on the grounds of size and/or activities.

   The IOC are in a position to take a pragmatic approach to compliance at organisations of all sizes (it is not uncommon for a company to tell the IOC that they will not be fully compliant by 25 May), however they are unable to scope out entities on the grounds of size or nature. The IOC has issued dedicated guidance for SMEs and other small organisations.

Some risks to think about

4. There was some concern that while the ICO currently sees itself as a pragmatic regulator, this may not always be the case. However, that the principles of proportionality are currently being applied by the courts is a mitigating factor; as is the expectation that the current Information Commissioner will be in role until July 2021. Some attendees also cited claim management firms and adverse media publicity as threats to the regulator's proposed pragmatic approach.

5. GDPR is not just a question of readiness for 25 May. The sustainability of data processes and data security is an ongoing issue and organisations should be careful not to exert a lot of energy to achieve compliance only for things to deteriorate thereafter. Thinking of GDPR as an enabler of innovation might help mitigate this risk.

6. Risks exist where the supply chain includes entities that are under invested in data protection – whether through lack of resources or otherwise. There is a danger that (say) SMEs may be cut out of the supply chain to reduce risk.

Turning a burden into an opportunity

7. GDPR is in many senses a burden on business, but the new processes and discipline required for compliance can create opportunities for businesses to build new and more profitable relationships with customers. For example, a number of retailers are seeking customer feedback at the same time as seeking consent. Similarly, staff training might re-kindle enthusiasm for looking at an organisation's business processes.

8. While there is a lot of focus on customers, the impact on employee information should not be forgotten. Prioritise the risks, but do not underestimate the sensitivity of employee data (salaries, illnesses, disciplinary matters, etc.) nor the degree to which records get shared with third parties.

The ICO website includes checklists, podcasts, worked examples and other guidance to help organisations across many different sectors. https://ico.org.uk/for-organisations/

Contact us

Timothy Copnell
KPMG Board Leadership Centre
T: +44 (0)20 7694 8082
E: tim.copnell@kpmg.co.uk