GDPR: MAKING A VIRTUE OUT OF A NECESSITY WHEN MANAGING DATA

A new forward-thinking approach to reduce risk of data breach has changed the way organisations view their processes in a drive to protect reputation

Since it came into force in May, GDPR has had a profound effect on the way that all organisations manage their data and relationships with customers. Issues that were once principally of concern to financial and regulated sectors are now affecting all industries. However, what was initially seen as a legislative burden has started to drive real business change and deliver tangible benefits.

The complexity of data and the increasingly varied ways in which it is used mean that managing it requires collaboration between DPOs and the business, legal, IT and information security among other departments. This is essential to mitigate privacy risks when developing products and services, to agree ethical approaches to data management and to protect that data. In many cases this involves a review of existing business structures, processes, culture and behaviour.

There are growing concerns among regulators, politicians and the public about how organisations manage customer data. Reducing the risk of a breach and reassuring audiences requires a more strategic approach, led by the C-suite.

Greater transparency of data

The cost of reputational damage is often considerably greater than fines, so organisations are having to work harder to communicate transparently about their data management procedures. They are using their highly ethical, forward-thinking approach and determination to go above and beyond what regulators require to create a positive brand image. Consumers, aware of the value of their data, are becoming more thoughtful about who they share it with and have higher expectations of transparent and ethical use of that data.

Beyond the EU, GDPR has created a ripple effect around the world with many other regions adopting similar privacy legislation. The California Consumer Privacy Act, for example, is due to come into force in 2020. In a drive to avoid a patchwork of regulations varying from state to state, the US may also consider a federal law, ensuring consistency across the US as GDPR has done for the EU. The APAC region has had data protection legislation for some time but there are moves to make it easier to share data across borders. Organisations which comply with GDPR will increasingly find they have the foundations for compliance with regulations in other territories.

When investigating there is a trend for regulators to undertake a thorough review of an organisation's data management and risk assessment procedures even when no external breach has occurred, as we have seen recently in Portugal. It is worth noting in the UK that most breaches reported to the ICO in the last quarter were caused not by malicious third parties but by inadequate policies and procedures in the organisation itself.

Monitoring internal processes

This means that as organisations work to protect their reputations and reduce the likelihood of fines or enforcement action and any reputational damage, their internal processes are increasingly critical.

The ICO is now more likely to ask about training, both for any individuals concerned with a breach and throughout the organisation.

As more companies look to operate like start-ups, increasing agility, their leaders need to help teams to be creative while complying with regulations.

One largely unreported consequence of GDPR is data minimisation – organisations are reviewing their policies to ensure they only retain data necessary for their operations and drive towards defensible disposal of data which has no retention requirements or business value. Not only does this minimise risk, it makes it easier to exploit data to drive strategic decision making and reduce storage costs and operational inefficiencies.

GDPR may have been the starting point, but as technology develops and customers get data-smart, all organisations will need to consider how they balance effective data governance with protecting the rights of individuals and delivering their marketing and brand strategies.

The key themes in this article were originally discussed in a panel moderated by Nina Bryant at the Managing Risk and Litigation Conference 2018, entitled 'What are the focus areas in 2019 and beyond on the proactive compliance agenda?' The panel members were: Michelle Levin, associate general counsel - digital and privacy, Coty; Jane Finlayson-Brown, partner, Allen & Overy; and Mo Ahddoud, chief information security officer, SGN

Nina Bryant, Director, information governance privacy and security practice

FTI CONSULTING

200 Aldersgate, Aldersgate Street, London EC1A 4HD
Tel: 020 3727 1124 **Email:** Nina.bryant@fticonsulting.com
Web: www.fticonsulting.com