CRITICALEYE
The peer to peer Board Community

A New Wave of Digital Trust

Nick Taylor, Managing Director for Accenture Strategy UK&I, tells **Marc Barber** why leaders need to carefully consider how they store customer data and the impact of the GDPR

In these data-obsessed times, it can appear like competitive advantage has been reduced to the speed at which a company can gather, analyse and then act on the information it has about its customers and employees.

This addiction to data will intensify as companies invest in artificial intelligence and the Internet of Things. It's predicted that the total amount of data stored globally is expected to rise from today's figure of 4.4 Zettabytes (ZB), to an estimated 35 ZB by 2020. To put this in context, it was around 0.7 ZB twenty years ago.

One of the challenges for companies is that in the excitement about what can be done with this information, it's easy to lose sight of the fact that a large portion of the data relates to real people, who are genuinely concerned about the control they have over their digital footprint.

Nick Taylor, Managing Director of Accenture Strategy UK&I, explains: "If you publish online or use social media, you will cast a digital shadow, which can be analysed in some way. Quite often, you won't realise you are doing this, and you'll also be unaware of how this information is being used.

"Even the things you think might be innocuous, such as photographs, can be analysed through facial recognition to identify friends and acquaintances. The location will also be noted so it's understood where you were when the photo was taken."

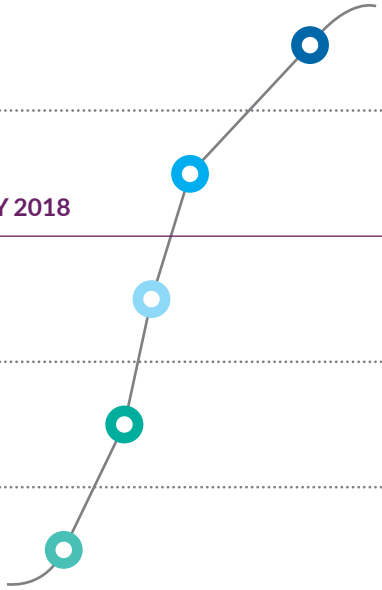
While it would be foolhardy for businesses to ignore data-driven commercial opportunities, it's equally true that CEOs and boards should think carefully about the privacy of the individuals they hold information on. **Nick** explains: "Not every customer or employee is comfortable with how this data is being used. I find myself having a lot of conversations with companies about the data they possess and what they do with this information – is it cool or is it creepy?"

Intrusive advertising is a growing problem for a number of customers. Within the workplace, there have also been instances of employees expressing concern over perceived breaches of privacy.

For example, at one media company, employees protested after finding devices attached to their desks which monitored activity levels. At another company, employees were given fitness trackers and some took offense when they received messages informing them to undertake more exercise.

When cyber crime is thrown into the mix, which is estimated to cost the global economy around $400 billion a year, it's understandable why regulators feel duty-bound to give people assurances >

Where are you on the GDPR Journey?



Journey Stage	Examples
OPTIMISING	• Leverage of secure personal data • Increasing trust with your customers • Breach rehearsal feedback loop
COMPLYING	• DPO and team in place as BAU • Privacy by design in all projects • Clear breach roles and responsibilities
REMEDIATING	• Integrated roadmap in place • Teams and projects delivering • Agreed remediation activities delivered
STARTING	• Programme of scoped activities developed • Estimates and budget approval • Priorities, partners and sponsors assessed
AWAKENING	• GDPR impact for your industry understood • Some understanding of gaps by division • Ownership mandated at the right level

about how personal data is managed. Individuals want to know where this information is being stored? Who is it being passed onto? Is it safe?

Dealing with Data

From May 2018, the European Union will require companies to provide answers to these questions and more with the introduction of the General Data Protection Regulation (GDPR). "The cool vs creepy discussion has always been on the table, because there is so much data that companies have on customers and employees," comments **Nick**. "The GDPR is forcing a different kind of conversation for businesses: is this information valuable or not?"

In practice, organisations need to rethink a wide range of processes and procedures to comply with the EU regulation. This includes putting a Data Protection Officer (DPO) in place if they are dealing with large volumes of information, as well as new restrictions on consent when profiling and acting on personal data. A lot of attention has also been given to organisations having to respond to a data breach within 72 hours – or run the risk of being fined either four per cent of global revenue or €20 million.

According to **Nick**, the full extent of the cost extends beyond these financial penalties. "If there is a breach and you're told you need to stop processing personal data until you have rectified the issue, the cost to the business is not just the regulatory fine. Rather, it's the cost of actually continuing to run your business."

The other key point to bear in mind, continues **Nick**, is that the regulation transfers power from businesses to people. "In this new world of the GDPR, individuals own their data, not the company," he explains. "As an individual, I can go to my bank and ask for the data they have on me and it will need to be handed over in an easily downloadable format.

"You can also request to find out how data is being processed and what decisions are being made. You then have the right to be forgotten, or the right to erasure, meaning that a company has to erase all of the data it has on an individual."

The scope and ambition of the GDPR may appear onerous, but **Nick** suggests it can be used as a means to gain a deeper understanding of customers and employees by building trust and developing better insights. "From an internal perspective, organisations can refocus on employees by looking at HR data, such as performance management, pensions, health, and all of the other support that is provided," says **Nick**.

In addition, **Nick** argues that the GDPR also creates the impetus for leadership teams to reassess existing customer relationships. He gives the example of an organisation mapping out 71 customer journeys, and discovering that 12 of these generated the most revenue. However, these were cross-divisional, so to maximise the opportunities they had to tie those journeys together.

So, are companies ready to comply with the GDPR? According to **Nick**, the answer is mixed. "Medical and pharma companies woke up to this quite early as they hold a lot of personal data. They were hot off the blocks when this was ratified in May 2016.

"Next, you saw banking, insurance and the telcos start to drive it hard, mainly before Christmas. Interestingly, retailers, utility companies and resources companies with a retail component, haven't been as proactive. Maybe it's because it's a year away, they're only just starting to think about it."

The EU's deadline is tight and therefore full compliance is unlikely for the majority of corporates, but that's not a reason to panic given the scale of the task to clean up data, as **Nick** explains: "If you won't be ready for May of next year, you should build a programme that is all about managing risks, listing them from the highest to lowest, and demonstrating where you are on the roadmap by the time you get to May 2018."

Nevertheless, executive and non-executive directors do need to be aware that the clock is ticking. ■

Nick Taylor
Managing Director
Strategy Lead, UK&I
Accenture Strategy

Nick leads the Accenture Strategy Group for the UK and Ireland. His experience includes business strategy and operating models, digital strategies and innovation, cost management, human capital management, organisational change and business transformation at huge scale.

Nick has worked with over 50 clients, including BBC, BP, Royal Mail Group, Korea Telecom, Vodafone and Marks & Spencer.

Contact Nick through:
www.criticaleye.com