On May 28, 2019, Ankura executives and legal experts took part in an industry webinar discussing the lessons learnt since the General Data Protection Regulation (GDPR) was implemented in May last year. In this article, we look at how global organisations are approaching an increasingly complex data privacy landscape as discussed in the webinar, which was attended by the following:

**Robert Bond | Partner**  
Bristows (host)

**Noriswadi Ismail | Managing Director**  
Data Privacy, Ankura;

**Richard Patterson | Managing Director**  
Cyber & Information Security, Ankura;

**Winnie Chang | Founder and Managing Director**  
OrionW.

**IS GDPR IMPLEMENTATION THE END OF THE STORY OR JUST THE BEGINNING?**

For many organisations, implementation was less challenging than they feared. As Robert Bond, Partner at Bristows and chair of the event explained, “Yes, business had to be more accountable. They had to be more transparent, but a lot of the building blocks were already in place.”

The bigger picture, however, is that many issues are not yet fully resolved. The detail surrounding the data organisations hold (whose it is, why it is being held, and how it is being managed)- not just across IT systems but also devices, messaging services, social media and more - is often not yet clear. The way that the GDPR bumps up against existing laws is also not fully resolved. Just one example is data retention, where other laws require data to be kept for longer than the GDPR demands.

Add to that the varying business imperatives, regional differences, and legal perspectives that impact on data privacy and in many ways the journey is just beginning. The positive here is that as these issues are addressed, better privacy models will emerge that not only aid compliance but also boost agility and support business growth.

**TAKING A GLOBAL APPROACH: A LEGAL PERSPECTIVE**

It could be argued that GDPR is already a global phenomenon because as we all know, it applies not only to organisations located within the European Union (EU) but also to those outside of it, if they market to or monitor EU data subjects. However, its global influence is spreading in other ways because it sets a benchmark that non-EU regulators are increasingly willing to match or even exceed.

One sign of this is new and emerging legislation such as The California Consumer Privacy Act and India's Draft Data Protection Bill. In addition, existing legislation is also being impacted, with established rules being adapted and extended.

**APAC aligns further with the GDPR**

As Winnie Chang, Founder and Managing Director of Singapore law firm OrionW puts it, “Lawmakers in the Asia Pacific (APAC) region have been busy analysing the GDPR and updating their own national protection regime.” For example, the Singapore government is bringing its Personal Data Protection Act (PDPA) more in line with the
GDPR by proposing three additional grants to extend the legal rights for processing personal data.

The first allows for an organisation to collect, use or disclose personal data as long as the affected individuals have been notified of the purpose for such collection, use, or disclosure, subject to certain conditions being met. The second allows for the collection, use, or disclosure of personal data without consent where it is necessary for a legal or business purpose, provided that the benefits to the public clearly outweigh any personal impact or risk to the individuals. An example of such legitimate interest would be prevention of fraud. The third, proposed most recently and with the consultation process still underway, allows organisations to use data without notice of consent — with certain limitations — if the purpose is to derive business insights and innovate in the development and delivery of products and services.

NEW APAC RULES ON DATA BREACHES
Currently, Singapore, unlike the EU, has no requirement for organisations to give notice of data breaches. That’s changing, however, with proposals to make it mandatory to notify individuals and the Personal Data Protection Commission (PDPC) of any data breach that poses a risk of impacting individuals. In addition, organisations must notify the PDPC where the scale of the data breach is significant, even if the breach does not pose any risk of impact or harm to the affected individuals.

EXTRATERRITORIALITY: IT WORKS BOTH WAYS
The global impact of the GDPR, such as on APAC businesses selling goods and services online to subjects in the EU, is well known. But what’s less well known is that it works the other way around too, and APAC’s data protection laws can apply to companies outside the region. For example, the laws in Australia, Singapore, and South Korea apply to foreign companies that collect or process personal data from citizens in those countries. The data protection laws of Japan and Malaysia also have some extraterritorial applications.

CLOSER ALIGNMENT OF GLOBAL PRIVACY DATA REGULATIONS
The big picture is that aligning non-EU privacy laws more closely with the GDPR, and the extraterritorial applications of both EU and APAC rules, is establishing a more level playing field for data privacy across different regions. Evidence suggests, however, that many differences and nuances are likely to remain for some time and will require specialist legal advice to navigate. This should not, however, prevent organisations from building a global framework for data privacy, but the key is to allow room for local alignment.

TAKING A GLOBAL APPROACH – THE COMMERCIAL VIEW
For commercial organisations, taking a global approach to data privacy goes beyond understanding the compliance needs of different geographies and jurisdictions. It is about taking into account every aspect of the business, from structure to culture and from company ERP systems to individual smartphones.

POST-MERGER CHALLENGES
To explain further, let’s look at the case of an organisation which, post M&A activity, now has its global HQ in California, plus regional HQs in London, Dublin, Singapore, and Kuala Lumpur. When this organisation originally did its GDPR assessment, its governance structure was very much centralised but, post-acquisition, activities are more varied with more business channels and third-party vendors. The challenge in this scenario is how to develop a global privacy framework.

There are several options. “A global CPO might prefer to stick to the GDPR framework, but legal counsel might prefer a local laws approach,” says Noriswadi Ismail, Managing Director, Data Privacy, Ankura. “Others may insist on an APAC approach within those markets rather than a global framework.” None of these options are wrong or right from a compliance point of view, but they are more about internal pressures. This neatly highlights how designing a privacy framework is not just about jurisdictions and compliance, it is about understanding the culture.
and structure of the organisation and then developing a solution that suits. That means connecting stakeholders, understanding that it is not all about technicalities, and working together to develop the right solution. Typically, that solution is a global framework with GDPR in mind, rather than a rigid centralised rule set. ‘Globally aligned, locally deployed’, is how it is sometimes summed up.

**PRIVACY IN HIGH RISK COMPANIES**

Case study number two involves an advertising technology sector dealing with data privacy. It is both complex and high risk because of the way personal data is shared with third parties, with other processors, and not just within the EU but outside of it as well. Given this situation, there is a real need to engage across all activities: with the relevant marketing people, data governance roles, data scientists, and the third-party vendors to really understand how they process and validate personal data. It is also necessary to continue validating the data flow. The point here is that it’s not enough to do basic GDPR compliance; organisations will need to take an all-round, global view of the data journey and treatment. In this case it was also necessary to engage with data protection authorities, with whom there was a lot of interaction and consultation. So, in this context ‘taking a global view’ has a slightly different meaning that goes beyond geography and jurisdiction to encompass all business activities and objectives.

**THE ROLE OF THE DPO**

Another key area is the role of the DPO across different regions and how they operate within a global organisation. In fact, even the job title itself is not globally applicable. In the US, the term is global chief privacy officer, which typically covers security as well as privacy. In the EU, the DPO is a statutory requirement with built-in independence but in Asia it’s different, with the DPO generally not a legal requirement. While understanding these differences, organisations should also focus on connection and integration. “By having greater interplay between CIOs, CTOs, DPOs and even CEOs, businesses will be more agile and better positioned to create successful global privacy frameworks,” says Noriswadi.

**WHEN GDPR COMPLIANCE GOES WRONG – DEALING WITH A BREACH**

Post-GDPR implementation, organisations are warier than ever about mass data breaches and the loss of personally identifiable information (PII) that could lead to regulatory fines and reputational damage.

As with most things in business life, preparation is key. So, what are the ramifications for an organisation facing a breach investigation by The Information Commissioner’s Office (ICO)?

The investigation will cover four areas: pre-attack controls, approach to risk, plus actual breach management, and corrective remedial action. The company would want the ICO to conclude that the control frameworks were adequate, the risk management approach was commensurate to the threats, the incident response was swift and effective, and that post-breach controls could prevent a repeat.

However, experience tells us that some of these four areas are more equal than others. Measuring the effectiveness of the control framework and approach to risk management, pre-breach, is more subjective and more difficult for the ICO. The other two, post-breach, areas are more objective and easier to measure. As Richard Patterson, Managing Director, Cyber & Information Security, Ankura says: “In my experience, the companies that get the breach management and the post-breach controls right are more likely to escape the fine. Get either of these two wrong and the overall finding is likely to go against the company.”

So, staying on the right side of the ICO will mean getting a good strategy in place for managing a breach and the right advice and organisational buy-in to learn lessons and ramp up controls to prevent future failures.

**‘WHAT, ME?’ THE DANGER OF ASSUMPTION**

From disgruntled insiders to criminal hackers and state actors, most organisations will be familiar with the list of potential attackers. They will also likely be aware of current cyber trends ranging from ransomware to phishing and email compromise. For companies that operate outside of high-risk sectors, however, like defence or phar-
ma, these threats can seem distant and it can therefore be hard for these companies to see themselves as a target. That could be a costly mistake because only a small percentage of attacks are now targeted. Even low-level cyber criminals now have advanced tools at their disposal which enable them to search broadly and opportunistically for weaknesses in systems rather than in specific companies. So, in a way, not being worried about cyber attack could actually make you a target.

BUSINESS AS USUAL?
The other risk is around dealing effectively with disrupted business continuity. A cyber attack can be devastating and result, perhaps, in losing all business communications and being unable to dispatch goods and services. Effective breach planning and good insurance will help, but it's important to be aware that an immediate return to ‘business as usual’ is unlikely. Instead, there needs to be compromise and sensible adjustment so that you can achieve your business needs within the necessary security arrangements.

In terms of getting that help, remember that many attacks are widespread and so you may not be the only organisation in need. Those with the expertise required to get you back ‘on the road’ will be in very short supply and insurance companies will likely have first call on their services. While having insurance can both help you in an emergency and show regulators that you are well prepared, from our experience, not all policies are the same. Companies must fully understand their own needs, their capabilities, and how they're going to respond. Then, they must make sure that the policy they select fully meets those requirements.

If you would like to discuss any of the subjects covered in this article or find out more about how Ankura can help you manage data privacy within your organisation, please contact noriswadi.ismail@ankura.com.

NORISWADI ISMAIL
Managing Director
+44 207 015 8740
noriswadi.ismail@ankura.com.

ABOUT US
Ankura is a business advisory and expert services firm defined by HOW we solve challenges. Whether a client is facing an immediate business challenge, trying to increase the value of their company or protect against future risks, Ankura designs, develops, and executes tailored solutions by assembling the right combination of expertise. We build on this experience with every case, client, and situation, collaborating to create innovative, customized solutions, and strategies designed for today’s ever-changing business environment. This gives our clients unparalleled insight and experience across a wide range of economic, governance, and regulatory challenges. At Ankura, we know that collaboration drives results.