AIG

The GDPR: Preparedness and Potential Impact in Asia

CONTENTS

THE GDPR: PREPAREDNESS AND POTENTIAL IMPACT IN ASIA

The European Union's General Data Protection Regulation (GDPR) was adopted in April 2016, and two years later, its enforcement date of May 25, 2018 is fast approaching. This new set of regulations will replace the Data Protection Directive 95/46/EC, harmonizing data privacy laws across Europe, while protecting residents' data privacy and transferring the power from organizations back to individuals when it comes to approaching and handling data privacy.

There are further-reaching implications as well. The provisions with regard to 'territorial scope' in the GDPR make clear that its requirements, in certain circumstances, apply to companies outside of the EU. In particular, the GDPR specifically applies to non-EU companies which:

(i) process personal data outside of the EU but in the context of the activities of their 'establishments' (for example, branches or subsidiaries) in the EU; or
(ii) offer goods and services to individuals in the EU; or
(iii) monitor the behaviour of individuals in the EU.

As such, non-EU businesses that process EU resident data will, in certain circumstances, be required to comply with European data protection law and appoint a representative to the continent. And since this regulation does not require national governments to pass any enabling legislation, like they would need to under a directive, the GDPR is directly binding and applicable upon its approaching enforcement date – enforcing a single, high standard for data protection across all 28 EU member states.

THE EVOLUTION OF THE GDPR

The Data Protection Directive 95/46/EC was introduced in 1995 to regulate the processing of personal data within the EU, making up an integral side of the EU privacy and human rights law. Thereafter, nearly two decades went by before there was an initial proposal for an updated data protection law by the European Commission (EC) on January 25, 2012. Over four years later, the GDPR was approved and adopted in April 2016, and enforcement will begin on May 25, 2018.

EU regulators saw the need for enhanced data protection regulations, as hacking scandals and increased online user data collection by advertising agencies and other organizations have led to rising public concerns over privacy. A growing number of high-profile security breaches, from Yahoo's announcement of having been the victim of the biggest security breach in history by a suspected "state-sponsored actor", compromising the security of 3 billion user accounts – to the eBay cyber-attack in May 2014 that saw names, birthdates and encrypted passwords of all 145 million users exposed. The hackers, eBay later admitted, were able to access the company network using the credentials of just three corporate employees, and managed to remain inside the system with total access for 229 days.

To fully understand the scope of the GDPR, it is important to understand what the EC recognizes as personal data. According to a 2012 press communication, the EC defines personal data as: "any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

The new rules will require many organizations dealing with EU residents to revisit what data they collect and how they collect it, while improving transparency about their usage of personal data. The GDPR makes it clear that organizations must only process data lawfully, fairly and in a transparent manner, only for authorized purposes, ensure data accuracy and integrity, not keep personal data longer than necessary, and implement appropriate data security measures.

One of the means by which an organization can demonstrate that its processing of personal data meets the "lawful" requirement, is by showing that consent has been sought and obtained from the data subject. The GDPR requires such consent to be freely given, to be requested from the data subject in a manner which is clearly distinguishable from other matters appearing in the same written declaration, and is presented in an intelligible and easily accessible form, using clear and plain language.

FINES AND NOTIFICATION

The GDPR brings with it penalties for non-compliance by organizations, including (for the most serious breaches) fines up to four percent of annual global turnover, or €20 million – whichever is greater.

The GDPR also specifies standards for breach notifications, wherein data processors in all member states where a data breach is likely to infringe on the rights and freedoms of individuals must notify their customers as soon as possible after first discovering an impending or already occurred data breach. Regulators must also be notified of the breach within 72 hours.

The GDPR also expands the rights of data subjects (i.e. the individuals about whom personal data relates) to more easily obtain data from the data controller regarding whether or not their personal data is being processed, and for what purpose, which must be provided by the data controller free of charge and, where the request is made by electronic means, in electronic format.

Data subjects are also entitled to the "right to be forgotten," which gives them the power to have the data controller delete their personal data. Conditions for data erasure do, however, need to be met, such as the data no longer being required for the purpose it was collected, or consent being withdrawn by the data subject.

Certain organizations will be required to appoint a Data Protection Officer, either an appointed staff member or external service provider, who should assist the organization to comply with data protection law and practices.

HOW WILL THE GDPR AFFECT BUSINESSES IN ASIA?

"Companies in Asia need to work out how the GDPR applies to them," explains Anna Gamvros, a Partner at global law firm Norton Rose Fulbright's Hong Kong office. "Given the global reach of companies in Asia, many could find themselves coming within the GDPR's scope and not even realising it. In essence, if an Asian business has any sort of footprint in the EU, or offers any goods services to individuals in the EU, or utilizes any form of monitoring which would include individuals in the EU, they need to consider whether GDPR will apply, even if it is a small company."

> The new rules will require many organizations dealing with EU residents to revisit what data they collect and how they collect it, while improving transparency about their usage of personal data.

Given the wide reaching implications of the GDPR, it is surprising that many companies in Asia may have overlooked the fact that the new regulations even apply to them. While companies in Europe have been making preparations for the past two years, many Asian companies are only just beginning to assess the impact of the GDPR.

"Amongst our clients in Asia, we are seeing varying levels of preparedness," comments Bhagya Perera, Director of KPMG's Cybersecurity Practice in Hong Kong. "Some have done nothing, most have started some sort of compliance project, and only a handful are truly ready for the GDPR."

GDPR ENFORCEMENT IN ASIA

The consequences for non-compliance with the GDPR can be steep – up to 4% of annual global turnover, or €20 million, whichever is greater.

However the question of how EU regulators will enforce the GDPR in overseas jurisdictions is less clear. Asian companies caught by the extra-territorial reach of the GDPR will (subject to certain narrow exemptions) be required to appoint a representative as a point of contact in Europe, which could be a local subsidiary or representative office. In these cases, regulators would most likely take enforcement action against this European contact if they have difficulty in taking action against the Asian company in question. The EU regulators may also look to work with Asian regulators to ensure effective enforcement.

RISING DATA SECURITY STANDARDS

"Although Asian privacy laws have definitely become more stringent in recent years, the GDPR is truly raising the bar on data privacy at a global level," Ms Gamvros continues. "There are many requirements to be fully compliant with the GDPR. We are working with our clients to prioritize certain aspects of compliance and to put in place an action plan to achieve full compliance."

With the GDPR setting the bar so high, many Asian companies assume that GDPR compliance will be sufficient to meet all other global requirements relating to data privacy and security. However in Asia's diverse environment, regulations can and do differ from jurisdiction to jurisdiction. Experienced global insurance, consulting and legal partners can help ensure organizations are fully prepared in terms of data privacy compliance.

"The application of the GDPR, for example, to companies anywhere in the world which offer goods and services to persons in the EU, means that this new law's impact outside of the EU and in the world at large will be considerable. Many Asian businesses look to the EU as a good source of customers. These businesses can either pay attention now, or potentially face paying a considerable price later," explains Jason Kelly, Head of Liabilities and Financial Lines for AIG in Greater China, Australasia and South Korea.

"In Asia, we have found relatively few companies are prepared for the GDPR, even though enforcement begins on a global scale in May 2018. With the deadline fast approaching, proactive companies are turning to experienced international insurers like AIG when seeking comprehensive solutions to address cyber exposure."

Beyond insurance coverage, multinational insurers offer a unique global perspective in conducting risk assessments for data breaches and other cyber attacks. Mr Kelly adds, "With a broad network of third party vendor relationships around the world, AIG offers particular strength in advising clients with operations in multiple countries – matched with comprehensive cyber coverage to offer a last line of protection against a rapidly evolving global threat."

JAPAN'S RESPONSE TO THE GDPR

Japan presents a unique market for GDPR compliance. As with many Asian countries, Japan found itself relatively late to the game in making preparations for the GDPR – with many Japanese companies not realizing the regulation applied to them until only recently.

In a survey of US, UK and Japanese companies conducted in June 2017, PWC found that only 22% of US companies had completed all preparations for the GDPR. In stark contrast, only 2% of Japanese companies had done the same. And in fact, the same survey found that 60% of Japanese companies had not even finished conducting impact assessments related to the GDPR, let alone made preparations for compliance.

According to Masumitsu Ito, Partner of KPMG FAS, "It is important for Japanese companies to assess if their operations expose them to the GDPR. For example, we have seen online banks in Japan that mainly target domestic consumers. With no

physical branches in Japan or Europe, they initially assumed their operations would not fall under the jurisdiction of the GDPR. However, as we looked into their business, we quickly realized that the bank kept records of financial transactions with entities in Europe, for example wire transfers – that include names, addresses and phone numbers – which meant they were exposed."

"Although Japan recently updated its Personal Information Protection Act (PIPA) in May 2017, PIPA and GDPR approach the protection of personal data from very different points of view. While the European regulation is more focused on data subjects' rights, the Japanese law looks more at the corporate side of data protection," explains Mr Ito. "A full assessment can help Japanese companies ensure they comply with both domestic and international data protection regulations."

"Many Japanese companies have fallen into the trap of thinking, 'This is a European regulation. As long as our European subsidiaries are in compliance, we are fine.' However, they may soon realize that data from these subsidiaries gets sent to other subsidiaries outside the EU, or back to headquarters in Japan. As a result, these entities must comply with the GDPR. If the data is sent to third party suppliers or outsourcing companies, these organizations must also now comply," adds Junichiro Uchiyama, Senior Manager of KPMG FAS.

Many Japanese companies appear to be unsure of how to approach the GDPR, and as a result have adopted a "wait and see" approach – choosing to see how other market players respond before taking action for themselves. However with GDPR enforcement slated for May 2018, time is running out.

A relatively underdeveloped risk management culture and comparative lack of experience in managing overseas risks are proving to be serious challenges for many Japanese organizations. At the same time, Japan is experiencing widespread market consolidation, with Mergers and Acquisitions (M&A) activity on the rise.

According to Mizuho Abe, Assistant Department Manager of Liability Financial Lines for AIG Japan, "As companies focus their efforts on post-acquisition business integration, efforts in risk management and data security have sometimes fallen by the wayside, leaving many Japanese companies exposed to data protection risks. In fact, a recent AIG survey found 70% of Japanese companies felt their cyber preparedness outside of Japan could use some improvement."

While many companies have expressed concern with the GDPR's tight 72-hour personal data breach reporting requirement, the challenge is magnified for companies operating across time zones. "For example, the time difference between a company's headquarters in Japan and its subsidiary in the EU would make coordination difficult – giving Japanese companies less time to assess the situation before having to file a report," explains Mr Abe.

In preparing to meet the demands of the new European regulations, many Japanese companies are finding benefits in working with multinational insurers and consulting firms. Mr Abe concludes, "AIG's multinational operations and global experience are proving useful for Japanese companies seeking to ensure GDPR compliance."

Mr Uchiyama summarises, "In the lead up to the GDPR's May 2018 enforcement date, we are advising all clients in Japan to conduct a thorough assessment of their operations to identify potential GDPR exposure. Find out if your business falls within scope of GDPR; and if resources are available, identify the risks and what must be done to rectify them. Consultants like KPMG with a broad range of international experience will bring definite advantages to the table."

"Many Japanese companies have fallen into the trap of thinking, 'This is a European regulation. As long as our European subsidiaries are in compliance, we are fine.' However, they may soon realize that data from these subsidiaries gets sent to other subsidiaries outside the EU, or back to headquarters in Japan.

WHAT SHOULD ASIAN COMPANIES DO BEFORE MAY 2018?

Although it remains to be seen how European regulators will begin to approach GDPR enforcement come 25 May 2018, companies in Asia that collect or process data from European customers should have a few preparations in place.

KPMG's Mr Perera clarifies, "We are advising clients in Asia to view the GDPR as an opportunity to identify and clean up personal data, and to ensure adequate data protection measures are in place. While we realize not every company in Asia will be fully compliant from the day of enforcement, it is important that they are at least aware of the requirements and ready to respond to requests from data subjects – for example regarding data removal or transfer." "Another important point for Asian companies that collect data from EU residents is that they must obtain data subjects' consent to store, process, transfer or sell their data. Companies must explain, in plain language, why they are collecting personal data and what they are going to do with it," advises Mr Perera.

GDPR PREPARATION CHECKLIST

Data audit
Understand what personal data your organization holds on customers, employees and partners – including how the data is collected and stored, and any third parties to whom it is transferred, especially noting any cross border transfers. This audit can be used to create the data processing records required under the GDPR.

Review consent
Review whether consent is required to process personal data or whether another legal justification may apply. If consent is required, ensure it meets the requirements of the GDPR.

Consider rationale
Consider and review the reasons for collecting, storing and processing personal data.

Update privacy notices
Under the GDPR, extensive information must be provided to data subjects, including details of the purpose of processing, legal justification for processing and an explanation as to their rights. This information must be concise, transparent, easily understandable and given in plain language. Review and revise privacy notices accordingly.

Data subject rights
The GDPR extends the information that must be given when an individual requests access to their personal data, and also creates new rights and enhances other rights – these rights include the rights of erasure ("the right to be forgotten"), rectification and restriction. Understand the data subject rights and ensure that your organisation can comply with them.

Appoint a Data Protection Officer
Companies whose core activities involve (a) large scale regular / systematic monitoring of data subjects or (b) large scale processing of 'special categories of personal data' (as defined in the GDPR and including health information) or criminal records data must appoint a Data Protection Officer (DPO). Ascertain if you need to appoint a DPO, and appoint one if required.

Reporting a data breach
Under the GDPR, EU regulators must be notified of a data breach within 72 hours if it is likely to result in a risk to the rights and freedoms of data subjects. Data subjects must also be notified individually where there is a high risk to their rights and freedoms as a result of the breach. Implement and test a personal data breach management and reporting policy and process.

Training
Staff must be provided with training on the GDPR so that they understand the impact on their work, and how and why the company retains information on their customers and employees.