Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

GDPR And APAC: 8 Letters Spell Out Major Changes

By **Samantha Green** (February 12, 2018, 11:59 AM EST)


Samantha Green

Thanks to better technology and the advent of the cloud, it is increasingly difficult for data to only live within an individual country's geographic borders. Alongside the mass collection of data comes culture differences on how it should be handled, secured and shared. With so much at stake and new privacy laws enacted each year, a single pool of data can often be governed by the laws of multiple countries. With mass globalization, more and more of these laws procured by each country need to be followed. In terms of compliance, multinational corporations operating in Asian and Pacific countries, which are some of the largest holders of data, will soon be saddled with not only the cumbersome laws enacted by China, Japan and Singapore, where many transactions take place in Asia, but also will likely need to comply with the European Union's new privacy directive. Any company that holds data of EU citizens, whether as consumers or business partners, will be required to improve their data privacy and security protocols to continue doing business with that part of the world. Navigating through all the laws can be an expensive endeavor, but noncompliance comes with massive risk. Monetary fines can bankrupt a company, and many businesses never recover from the tarnished brand image.

The General Data Protection Regulation (GDPR), which will take full effect in May 2018, introduces a single set of rules relating to collection, storage and processing of personal data across the EU. These rules apply to both organizations in the EU (regardless of whether the processing takes place there) as well as all organizations that processes the personal data of subjects in the EU related to offering goods or services in the EU or monitoring their behavior within the EU.

Privacy in the EU is of paramount importance, and the GDPR was enacted to ensure each individual's data, no matter how collected, is secure and private. Therefore, all organizations must have processes and procedures in place to safeguard personal data, which means recording what personal data they have, where it comes from, who it's shared with and what they do with it. It further requires them to audit information to map data flows and maintain records of the legal bases of processing.

One of the newest and toughest burdens the GDPR will place on all organizations is that when a breach occurs, the company must report the breach to the proper authorities in 72 hours (Article 33(1)). When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller is also required to notify the affected individuals "without undue delay" (Article 34). If a breach is not reported in the 72-hour window, a fine of up to 20,000,000 euros or up to 4 percent of

total worldwide turnover of the preceding year, whichever is higher, can be levied (Article 83(5)).

The rules are very specific as to how a breach must be handled, and every company dealing with an EU citizen's data must be prepared to provide the following information in the prescribed 72 hours. A notification to the proper GDPR authority must "at least":

1. Describe the nature of the personal data breach, including the number and categories of data subjects and personal data records affected,
2. Provide the data protection officer's contact information,
3. Describe the likely consequences of the personal data breach,
4. Describe how the controller proposes to address the breach, including any mitigation efforts. If not all information is available at once, it may be provided in phases.

No APAC country has such a strict, defined timeframe. Network operators in China that hold the strictest standards in the APAC, under the Cybersecurity Law must promptly inform data subjects if their personal information is disclosed, tampered with or destroyed, and notification must also be made promptly to the relevant authorities. However, there is no definition of what "promptly" means in terms of timeline, and no specifically defined fines assessed for not reporting in a certain timeframe. In Japan, Hong Kong and Singapore, there is no explicitly required notification to a ministry or governmental authority in the event of a leak or security breach. Since APAC businesses have not had to detect a breach and report in such a tight timeframe, many businesses may be unprepared for this hurdle.

What APAC Businesses Can Do to be Able to Comply with the GDPR Breach Notification Requirement

Asian companies that need to comply with the GDPR must now have extremely tight control of their data, invest in necessary infrastructure and software to prevent a breach, and have internal policies and procedures in place to deal with a breach so it is noticed early and acted upon right away.

To do this requires a coordinated approach, including technology, breach response policy and training. This can be a big investment in both time and money.

First, there are certain technological requirements that must be in place to be GDPR compliant. These will vary for every organization but will usually include firewalls, log recording, data loss prevention, malware detection and similar applications. There are many other sophisticated applications that can spot when unusual activity on a corporate network occur. At a high level, APAC businesses should focus on determining which data contains sensitive information and ensuring those are protected. Data encryption still can be highly effective even when the underlying technology is not cutting edge, and data masking, a technique that uses substitute characters to avoid exposing actual data values, can also prove very useful in protecting sensitive data. An investment in technology to protect personal data is unfortunately not a one-time expense, but it is an ongoing investment to keep up with sophisticated hackers and to avoid negligent behavior by internal personnel.

Second, in conjunction with technology, breach response procedures must be put in place so that when a red flag is raised by one of the internal detection programs, an established plan alerts the proper people who can take steps to stop the breach and report it to the proper authorities in a timely fashion. An effective breach response requires a combination of skill sets, including IT, PR and legal. The plan should include standard notification procedures. There must be guidance for how to develop internal operations for detection, categorization, investigation, containment and reporting of data breaches. Since networks are under constant attack, there needs to be a hierarchy in place so that more serious

breaches are focused on first.

Third, APAC businesses looking to satisfy GDPR standards will also need to ensure that staff is properly trained on security protocols. Regular staff training is essential to raise awareness of the importance of good security practices, current threats and whom to call if a breach is suspected. It is also important to avoid a blame culture that may deter staff from reporting breaches.

Conclusion

With many APAC businesses having a presence in multiple countries, they already need to comply with many country-specific regulations. Adding the GDPR to the mix certainly makes things even more cumbersome, especially when the cost of violation is so high. With no guidance yet on enforcement of the GDPR, businesses are left to navigate unchartered dangerous waters, as one violation could cost a company up to 4 percent of their annual gross profit and significant reputational harm.

Samantha Green is the manager of thought leadership for Epiq Systems Inc. She has more than 15 years of litigation and consulting experience, has published numerous articles and white papers, and has authored chapters for ABA, Inside Counsel and West publications. She has spoken all over the country and provided more than 100 CLEs on topics relating to e-discovery, litigation readiness, international data privacy and case law.