Data Protection and Privacy Key Trends & Developments Affecting Asia

Charmian Aw, Counsel at law firm Reed Smith, deduces that the proposed changes to India's data protection legislation will have a significant impact on the broader universe of data privacy and compliance for the rest of Asia. She told the audience at the Hubbis Compliance in Asian Wealth Management Forum in Singapore that as so many Asian economies are focussing heavily on the digital economy, more comprehensive and stringent data privacy legislation is inevitable.

Link to Content Summary page
Link to Article on website
Link to Presentation
Link to Event Homepage

"THIS IS A HOT TOPIC," Aw began. "Data," she told the assembly, "is innately and increasingly valuable to your business, to your clients, to individuals, and therefore we see an increased spotlight globally on data and data protection, as well as cyber security and Asia is certainly no exception."

A bird's eye view of Asia

She gave a swift overview of Asia, noting its diversity. Many of the

CHARMIAN AW
Reed Smith

region's leading economies – Singapore, Hong Kong, Malaysia, the Philippines and others - have personal data protection legislation, albeit to differing degrees, while countries such as Cambodia, Myanmar, Laos, Vietnam, Indonesia, Brunei, and India are still to introduce their new legislation.

"This is why we are in such exciting times," Aw commented, "because many of these countries have drafted legislation that is soon due to be implemented. For example, China might not have all-encompassing data protection legislation, but they do have the Personal Information Security Specification, which although not legally binding does guide how the government agencies will enforce data protection in China."

India in the spotlight

Aw explained that she would in her presentation focus on India and extrapolate general rules and lessons from that vast, rapid growth economy. "India," she observed, "is at a fascinating turning point because they will soon pass their first ever, overarching data protection legislation, perhaps before 2019 is out. Right now, there might be some laws covering data and data protection, for example, the Information Technology Act 2000, but there is no overarching comprehensive legislation on data privacy, akin to Singapore's Personal Data Protection Act, as yet."

She took a step back to observe the origins of current legislation around the world. "For example, Europe's GDPR is closely linked to human rights laws. In the US, consumer rights and consumer protection laws are key drivers. In Singapore, there is no emphasis on a constitutional right to privacy or the right to personal data protection per se, whereas in India, Article 21 of the Indian Constitution does prescribe a fundamental right to individuals to protect their personal liberty."

India – a "fourth" way of regulating data protection

Aw then mined down in some detail to the essential elements of the new Indian legislation. "When this law comes into force it will accord basic rights to individuals concerning their data," she reported. "There will be compliance obligations imposed on businesses that have Indian operations. And it proposes what we can call a 'fourth way of regulating data protection on top of what the US, the EU and China have introduced or proposed. We see that there are data principals, for example, the individuals, employees, business associates. And there are the data controllers, which India will term data 'fiduciaries', the word implying that businesses that operate in India must adhere to the concept

of trust when handling the data of the principals."

Oversight and enforcement will be handled by the Data Protection Authority of India (DPAI) who will levy a series of penalties and financial fines for non-compliance. Fines, she explained, could be very high - even up to 4% of worldwide turnover. "The good news for the fiduciaries is that there will be a sunrise period after the passing of the act and before the full implementation, therefore giving the fiduciaries the time to align their practices and policies."

There will also be specific rights and even certain obligations on the principals. For example, they will have the right to ask the fiduciaries how their data is being used, but also a responsibility to ensure that the information they provide is accurate.

Aw explained that India would also legislate for the right of data portability. This portability is required in Europe, allowing the data principals to demand that fiduciaries pass their data to another service provider without any strings attached and without retaining any such data. Additionally, annual data audits will be required and must be handled by law by data auditors.

"I should mention that India is quite forthright in all this, for example, the right to be 'forgotten' will also be included in the Indian act, which is the right to have data deleted or erased from public record."

India's extensive data net

As to the net cast by the new Indian legislation, Aw explained that it covers any business with a physical presence or registration in India, any company whose systematic activity involves offering goods and services to data principals who are individuals in India, or any party performing any activity that involves profiling of data principals within the territory of India.

Aw also noted that every data fiduciary would need to appoint a DPO, which is a Data Protection Officer. And organisations not physically present in India but still under the scope of the new act must appoint a DPO that is based in India.

Conclusion

Aw drew lessons from the developments taking place in India. "First, anyone operating in India or linked to India must position themselves for these new, highly robust laws and practices. Secondly, think about data minimisation, meaning do not over-collect data, do not retain data unnecessarily, and regularly purge data you do not require. Think about your data protection impact assessment and make sure that your products and services always have privacy embedded in them. In brief, remember that the proliferation of new data regulations and compliance requirements mean assessment and action are both essential." ■