



Andrea Jelinek, the head of the European Data Protection Board (EDPB), which is a new European body created to enforce GDPR.

PHOTO: REUTERS

Asean-India need to respond to GDPR in Europe

Trade pacts with the EU may see provisions of its General Data Protection Regulation being incorporated into them. **By CHAN JIA HAO**

IN THE last eight years, more than 7.1 billion identities were found to have been exposed in data breaches worldwide. In a timely response, the European Parliament approved the General Data Protection Regulation (GDPR) in 2016. This regulation, under the European Union (EU) law, attempts to harmonise and govern data protection and privacy for all individuals within the EU and European Economic Area.

The GDPR became enforceable on May 25, 2018, and applies to any organisation that processes personal data of individuals in the EU, including organisations that have permanent establishments outside of the EU. This is so long as there is the offer of goods or services to individuals in the EU, or that the organisation is involved in monitoring the behaviour of individuals in the EU. In particular, the GDPR calls for fine impositions of up to 20 million euros (\$31.7 million) or up to 4 per cent of an organisation's annual global turnover, depending on the provisions infringed upon.

Companies across India and South-east Asia with dealings with the EU have taken the first step towards compliance by changing their privacy statements. They include operators in the entertainment and tourism industry, the financial, healthcare and retail sectors, mobile app developers and non-profit organisations.

Indeed, data privacy concerns could impact economic cooperation in this region, particularly between the Association of Southeast Asian Nations (Asean) and India in terms of digital connectivity. This is because exchanges of data are becoming one of the most important drivers in today's bilateral e-commerce and e-governance exchanges. This is coupled with the growing importance of a combined India-Asean information and communication technology

(ICT) sector market demand projected to grow to US\$9.4 trillion (\$12.8 trillion) by 2020.

Currently, however, data protection is a fragmented theme within and across Asean and India. Myanmar, Laos, Cambodia and Brunei do not possess any legislation in data protection and privacy. Thailand, on the other hand, is only now in the midst of passing its Personal Data Protection Bill which was first proposed in 2011.

The other Asean member states possess data privacy laws, for example, Singapore (Personal Data Protection Act 2012), Malaysia (Personal Data Protection Act 2010), Indonesia (Law of the Republic of Indonesia Number 11 of 2008), Philippines (Data Privacy Act of 2012) and Vietnam (Law on Protection of Consumers' Rights 2010). India too has such laws in place, notably, the Information Technology Act 2000.

However, the liberalisation in cross-border data exchanges across these countries differs. For instance, India's IT Act 2000 limits cross-border data exchange unless the individual's consent is obtained. At the other end of the spectrum, Singapore is looking at allowing certified organisations to exchange personal data with other such organisations in participating Asia-Pacific Economic Cooperation (Apec) economies, as part of Singapore's participation of the Apec Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors systems. Singapore is currently the sixth Apec economy to have joined the CBPR system, along with the US, Mexico, Canada, Japan and South Korea, while its fellow Asean member states and India have not done so.

At present, Asean countries such as Singapore, Malaysia and the Philippines provide for data protection of general application. Under its IT Act 2000, India has

also punishments in place for non-compliance, with the most severe being up to seven years of imprisonment and/or fine of up to 1 million rupees (\$19,860).

On the European Commission's end, there has been an endorsement of horizontal provisions in January 2018 for cross-border data flows and personal data protection in trade negotiations.

Under these provisions, the Commission, as a result of treating the protection of personal data as a fundamental right in the EU, can only allow data flows between the EU and third countries with mechanisms provided under the EU data protection legislation.

This implies that, ultimately, bilateral and multilateral free trade agreements (FTAs) with the EU, including the EU-Asean FTA, may see the parameters of the GDPR being re-incorporated into them. With this, the EU could make its data protection scheme a trade-off in its economic relations. Nonetheless, Asean, as a bloc, must first reach consensus on its data protection standards. This is also a need for Asean to convince India, one of its regional trading partners, that the regional grouping is transforming itself into a single market with standardised market facilitation rules.

Only then can both sides effectively proceed with norm settings on the data protection front, either bilaterally or at the Regional Comprehensive Economic Partnership level. The task could be made even more difficult if some countries, which do not have stringent data protection laws, allow permanent establishments within their territories to enjoy lower standards in data protection compliances.

The European Commission has already seen investigations in a few EU-member states on breaches in EU antitrust rules. Competing services providers in these countries were investigated for working together to share bank account information of their customers.

If such a phenomenon ensues in Asia, cross-border data exchanges can surge among those countries that do not have comprehensive data protection. Conversely, those with stronger data protection may be seen as ring-fencing themselves from the rest. Such a political economy would be inconsistent with the discourse of regional economic integration and cooperation. Therefore, Asean and India – as they seek to further their ICT cooperation – must step up their data protection standards across the board.

■ The writer is a research assistant (trade and economic policy) at the Institute of South Asian Studies, National University of Singapore.