ISAS Brief
No. 584 – 20 June 2018
Institute of South Asian Studies
National University of Singapore
29 Heng Mui Keng Terrace
#08-06 (Block B)
Singapore 119620
Tel: (65) 6516 4239 Fax: (65) 6776 7505
www.isas.nus.edu.sg
http://southasiandiaspora.org

The European Union-based General Data Protection Regulation: Implications for India and ASEAN

Chan Jia Hao[1]

The General Data Protection Regulation (GDPR) is a regulation law that governs data protection and privacy for all individuals in the European Union (EU) and the European Economic Area. The GDPR was adopted in 2016 and became enforceable in May 2018. The regulation saw many private companies and websites worldwide change their privacy statements due to fears of data breaches resulting in heavy economic sanctions. While there is concern among private corporations that the EU-based GDPR standards will impose heavier data privacy regulations here in Asia, the current differences in the level and scope of data privacy standards in India and the Southeast Asian countries reveal a low level of readiness to embrace regional information and communications technology (ICT) cooperation. In the case of ICT cooperation between India and the Association of Southeast Asian Nations (ASEAN), whether this non-standardisation could limit future cross-border e-commerce and e-governance exchanges depends highly on the next course of action by India and ASEAN.

[1] Mr Chan Jia Hao is a Research Assistant (Trade and Economic Policy) at the Institute of South Asian Studies (ISAS), an autonomous research institute at the National University of Singapore (NUS). He can be contacted at chanjiahao@nus.edu.sg. The author bears full responsibility for the facts cited and opinions expressed in this paper.

In the last eight years, over 7.1 billion identities were found to have been exposed in data breaches worldwide.[2] While countries in the European Union (EU) have long possessed data protection legislations, with a notable example being Ireland's 1995 Data Protective Directive, the European Parliament approved the General Data Protection Regulation (GDPR), known as (EU) 2016/679 in 2016.[3] This was in response to the magnitude and increase in data breaches. This regulation, under the EU law, attempts to harmonise and govern data protection and privacy for all individuals within the EU and European Economic Area.

Scope and Enforceability of the GDPR

The GDPR became enforceable on 25 May 2018. Under Article 3, the GDPR applies to any organisations that process the personal data of individuals in the EU, including organisations that have permanent establishments outside of the EU.[4] 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.[5] Aside from outlining lawful procession of personal data, rights of individuals, accountability and governance and data breach notification procedures, Article 83 – Administrative Fines of the GDPR calls for fine impositions of up to €20 million (S$31.3 million) or up to four per cent of an organisation's annual global turnover, depending on the provisions infringed upon.

As a result, companies across India and the Association of Southeast Asian Nations (ASEAN) with dealings with the EU have taken the first step towards compliance by changing their privacy statements. The number of parties is wide ranging. They include the entertainment and tourism industry, the financial, healthcare and retail sectors, mobile app developers and non-profit organisations, as well as those who deal with personal data of EU individuals. In such a case, data privacy concerns could impact economic cooperation among countries in

---

2 Brian Fletcher. 'How new EU data protection law will impact Singapore firms.' *Business Times* https://www.businesstimes.com.sg/opinion/how-new-eu-data-protection-law-will-impact-singapore-firms. Accessed on 19 June 2018.

3 Background and Introduction to the General Data Protection Regulation. https://www.lexology.com/library/detail.aspx?g=d7f59709-4362-4155-ab6f-de55af4147a4. Accessed on 19 June 2018.

4 Ibid.

5 Personal Data Protection Commission Singapore - European Union General Data Protection Regulation Factsheet for Organisations. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/eu-gdpr-factsheet--041017.pdf. Accessed on 19 June 2018.

this region, including between ASEAN and India, particularly in digital connectivity. This is due to the exchange and application of big data becoming one of the most important drivers in today's e-commerce and e-governance exchanges.[6] This is particular so, given that India-ASEAN combined information and communications technology (ICT) sector market demand is projected to be more than US$0.94 trillion (S$1.28 trillion) in 2020.[7]

Differences in Level of Data Privacy Protection in ASEAN and India

Currently, there are differences in the level and scope of data privacy standards in India and the Southeast Asian countries. Among the eleven countries in the region, Myanmar, Laos, Cambodia and Brunei do not possess any legislation or draft legislation in data protection and privacy.[8] Thailand, on the other hand, is in the midst of passing the Personal Data Protection Bill 2011 which was first proposed in 2011.[9] This is despite the existence of a Framework on Personal Data Protection at the ASEAN level, which is modelled after the Asia-Pacific Economic Cooperation (APEC) forum Privacy Framework (2015). It is aimed at enabling the ASEAN-member states harmonise a framework on personal data protection consistent with the ASEAN ICT Masterplan 2020.[10]

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, for example, the Information Technology Act 2000. However, the timeframe of the implementation and liberalisation of cross-border data exchanges are fragmented. For instance, India's Information Technology Act 2000 under the Ministry of Electronics and Information Technology limits cross-border data exchange unless the

6 Chan, Jia Hao. 2018. ASEAN-India Cooperation in Information and Communications Technology. https://www.isas.nus.edu.sg/wp-content/uploads/2018/05/ISAS-Insights-No.-493-ASEAN-India-Cooperation-in-Information-and-Communication-Technology.pdf. Accessed on 19 June 2018.

7 Ibid.

8 Latest data protection and privacy legislation worldwide database from UNCTAD.

9 Simon, Chesterman. 2014. Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World.

10 ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) Framework on Personal Data Protection.http://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf. Accessed on 19 June 2018.

individual consent is obtained.[11] At the other end of the spectrum, Singapore is looking at allowing certified organisations to exchange personal data with other certified organisations in participating APEC economies as part of Singapore's participation in the APEC Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors systems.[12] Currently, Singapore is the sixth APEC economy to have joined the CBPR system along with the United States, Mexico, Canada, Japan and the Republic of Korea, while its fellow ASEAN-member states and India have not done so.[13]

What's next for ASEAN and India in the face of the GDPR?

On the collective ASEAN end, the current Framework on Personal Data Protection does not mention the implications of non-compliance, as compared to the GDPR. However, countries such as Singapore, Malaysia and the Philippines provide for data protection of general application.[14] Under its Information Technology Act 2000, India has punishments in place for non-compliance, like the GDPR, with the most severe being up to seven years of imprisonment and/or a fine of up to 1 million rupee (S$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 flow between the EU and third countries with mechanisms provided under the EU data protection legislation.[15] This implies that, ultimately, bilateral and multilateral free trade agreements (FTAs) with the EU, including an upcoming EU-ASEAN FTA, may see the parameters of the GDPR being re-

[11] Joshua P. Meltzer, and Peter Lovelock. (2018). Global Economy & Development Working Paper 113, Regulating For A Digital Economy, Understanding The Importance of Cross-Border Data Flows In Asia. http://trpc.biz/wp-content/uploads/digital-economy_meltzer_lovelock_web.pdf. Accessed on 19 June 2018.

[12] Ministry of Communications and Information – Singapore Joins APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems. https://www.mci.gov.sg/~/media/mcicorp/images/budget%20workplan/cos%202018/factsheets/factsheet%20-%20singapore%20joins%20apec%20cross-border%20privacy%20rules%20and%20privacy%20recognition%20for%20processors%20systems.pdf?la=en. Accessed on 19 June 2018.

[13] Ibid.

[14] Impact of the EU General Data Protection Regulations on ASEAN Businesses. http://zico.group/wp-content/uploads/2018/04/ZICO_10-10_GDPR-2018.pdf. Accessed on 19 June 2018.

[15] European Commission – Daily News 31/01/2018. http://europa.eu/rapid/press-release_MEX-18-546_en.htm. Accessed on 19 June 2018.

incorporated into them. The India-EU FTA is also currently under negotiation. India is the EU's 9th and 10th largest trading partner for the EU's imports and exports respectively as of 2017.[16] In such a scenario, the EU could make its data protection scheme a trade-off in its economic relations. It appears that, for private entities and governments across ASEAN and India, the impact of the EU-based GDPR has already taken place, at least in self-initiated legal compliance. This is due to the fact that the EU remains an important market for both ASEAN and India.

Nonetheless, it remains to be seen if the differences in data protection standards across the ASEAN-member countries and India will see them harmonise and upgrade the stringency on data protection so as to bring them closer to the EU-based GDPR standards. ASEAN, as a bloc, must first reach consensus on its data protection standards. This is not easy, given their differing standards. However, the task would be made more difficult, if some countries, which do not have stringent data protection laws, allow permanent establishments[17] within their shores, to pass their lower standards in data protection compliances. The European Commission has already witnessed investigations in a few specific EU-member states on breaches in the EU Antitrust rules.[18] Competing services providers in these states were investigated for working together to share bank account information of their customers.

If such a phenomenon replicates itself among countries in Asia, cross-border data exchanges can surge among those countries that do not have comprehensive data protection. Conversely, those with higher data protection may be seen as ring-fencing themselves from the rest. Such a political economy is inconsistent with the discourse of regional economic integration and cooperation. Therefore, ASEAN and India must ensure that they steer clear of this course to ensure progressive development in ICT cooperation between them.

. . . . .

[16] India-EU – International Trade in Goods Statistics. *Eurostat*. http://ec.europa.eu/eurostat/statistics-explained/index.php/India-EU_%E2%80%93_international_trade_in_goods_statistics#EU_and_India_in_world_trade_in_goods. Accessed on 19 June 2018.

[17] A permanent establishment largely refers to a fixed location of a business entity in a specific jurisdiction. Depending on individual jurisdictions, this may cover warehouses, factories and places of management of the business entity. The term is commonly used in the field of international taxation for matters relating to double taxation and registration formalities.

[18] European Commission – Fact Sheets: Antitrust: Commission confirms unauthorized inspections concerning access to bank account information by competing services. *European Commission Press Release Database*. http://europa.eu/rapid/press-release_MEMO-17-3761_en.htm. Accessed on 19 June 2018.