Data Privacy as a Competitive Advantage

Data privacy as a competitive advantage

TRPC

Briefing Paper
2nd November 2018

Table of Contents

Background 3
Personal Data Privacy Policies 4
Technology, Business Models and Personal Data Privacy and Protection 5
The Implications 6
The Complexity: In brief, what is new about GDPR? 7
Cost of Compliance 8
Cross-Border Data Flows 11
Thailand's Personal Data Protection Bill 13
Implications of the PDPB 14
Additional Resources 16

Background

In 2016, the European Union (EU) Member States issued a new body of rules on data protection – the General Data Protection Regulation (GDPR), which came into force on 25 May 2018. The GDPR is considered an urgent update to the EU's 1995 Data Protection Directive in light of rapid advances in technology and emergent business models. Until everything went digital, the collection of data about individual persons was mostly done by governments, education and health services, utility companies and banks. Sometimes retailers would gather personal data in pursuit of loyalty schemes, but in none of these cases was the objective seen to be the sale of that data to others. Digital changed all of that, making data easy to collect, store, analyse, and transfer in a cost-effective way. The advent of the World Wide Web gave rise to new costless ways to collect data (*click through*) on mass, just as connectivity through the Internet multiplied the opportunities to transfer that data (*network effects*). The decisive shift from an arithmetic to geometric progression of data generation and capture was the advent of the smartphone, and the decisive mechanism has been users giving access to their contact lists – without the contacts ever knowing their data is being handed over; they have become part of the growing mash-up.[1] Absence of contact sharing would take social media applications much longer to build their critical mass. The challenge in protecting data is yet further exacerbated when digital services are provided across national borders and across jurisdictions.

> "Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location."[2]

The extra-territoriality of GDPR, one of the fundamental attributes of the new regulation, is aimed at understanding and tackling cross border trade and data flows. Previously, the jurisdiction was confined to the location of the data subject, however under the GDPR, this now extends to include the location in which a consumer's data is being stored and/or processed. This implies that companies involved in the transfer of data from any resident of the EU, must not only operate in jurisdictions that are considered the equivalent to the EU in terms of data privacy regimes, but should also be compliant to the standards set by the GDPR, especially with respect to data protection and security. This includes organisations which are not established in the EU, but which offer goods or services to individuals in the EU, or which monitor the behaviour of individuals in the EU. The GDPR applies to any data controller or data processor that has even a minimal presence in the EU. The interpretation of minimal would seem to mean any stable or lasting presence, however small.[3] So, for example, any Thailand-based organisation, such as a hotel, bank, insurance company, and e-commerce websites that offer goods or services to individuals located within the EU and have a representative of any kind in the EU, will have to ensure that their practices and processes are compliant with the GDPR. Failing which, there is the risk that they will be subject to the penalties. This framework of extra-territoriality applicability for personal data occurring in Thailand has also been introduced in the Thai Personal Data Protection Bill (PDPB).

[1] Mash-ups are often defined by the type of content that they aggregate. A content mash-up, for example, brings together various types of content for presentation through an interface. That content could include -- among other things -- text, data feeds, video and social updates. An enterprise mash-up typically combines internal corporate data and applications with externally sourced data, SaaS (software as a service) and Web content. Business mash-ups might also provide integration with the business computing environment, data governance, business intelligence (BI)/ business analytics (BA), more sophisticated programming tools and more stringent security measures. https://whatis.techtarget.com/definition/mash-up

[2] https://www.eugdpr.org/key-changes.html

[3] https://www.quora.com/Does-the-GDPR-apply-to-US-companies

Personal Data Privacy Policies

Emerging technologies and changing business models that make primary use of data have driven governments to introduce and update personal data privacy laws, but this legislative process is often lengthy and has not kept pace with digital transformation. The focus of personal data privacy policies however, varies according to the dynamics of different jurisdictions where the absence of homogeneity in updating data protection laws has hindered international harmonisation of regulations.

In the EU the focus is on the harmonisation of laws and regulations across the region, and an emphasis upon the privacy and security of personal data, as ultimately judged by the European Court of Justice. For example, as demonstrated by the enhanced 'data protection by design' security provisions of the GDPR, which relate specifically to companies that build their business on data collection and usage. In Asia Pacific, the Cross-Border Privacy Rules (CBPR) of the Asia-Pacific Economic Cooperation (APEC) are principally designed to safeguard personal data privacy as an assurance of cross-border data flows and international trade, which is the lifeblood of 21-member economies.

In the US, the focus is on pro-business private-sector self-regulation, with notable differences in laws (or the absence of laws) across different states. Under pressure to assure cross-border data flows with the European Union (EU), the US agreed to a Privacy Shield – a replacement to the Safe Harbour agreement – under which the Federal Trade Commission (FTC) will police the workings of self-regulation.[4] This arrangement however, is already being challenged by Max Schrems, a young Austrian lawyer, and other data rights groups.[5]

The basis of these challenges centre around two sets of issues: access by the US government to personal data over the Internet and personal data held by private companies – this became a highly sensitive issue following the revelations of Edward Snowden and the PRISM mass surveillance programme[6] – and the level of transparency of social media companies and others. The final judgement of the European Court of Justice in 2015 on the Safe Harbour agreement "found that the framework is invalid for several reasons". It was found that the Safe Harbour agreement compromised EU citizens' right to respect for private life, compromised the fundamental right to effective judicial protection, and denied national supervisory authorities their powers to investigate breaches of the principles behind data protection.[7]

Most recently the EU signed an agreement with Japan that recognises each other's data protection rules as adequate and sufficient insofar the comparable levels of safeguards and protection of personal data allow for the transfers of personal data between both countries.

Box 1: EU Signs 1st Reciprocal Data Privacy Deal with Japan

The EU and Japan have agreed to formally recognise each other's data protection rules as part of the free trade agreement signed on the 16th June 2018.[8] Under the newly inked deal, organisations can now transmit personal data of its data subjects between the EU and Japan without the requirement of any particular authorisation. These companies are however still required to observe the existing regulations from either the EU or Japan.

[4] http://europa.eu/rapid/press-release_IP-16-216_en.htm For a useful comparison, see https://www.twobirds.com/en/news/articles/2016/global/safe-harbor-replacement-approved-by-european-commission
[5] https://iapp.org/resources/article/a-brief-history-of-safe-harbor/
[6] https://en.wikipedia.org/wiki/PRISM_(surveillance_program)
[7] https://www.scmagazineuk.com/updated-safe-harbour-ruled-invalid-european-court-justice/article/1479260
[8] http://europa.edu/newsroom/rapid-failover/ip-18-4501_en.pdf

This is the first time that the EU and a country from Asia Pacific have agreed on a reciprocal recognition of the adequate level of data protection. Currently, the EU has adopted only unilateral adequacy decisions with 12 other countries – namely, Andorra, Argentina, and Canadian organisations subject to The Personal Information Protection and Electronic Documents Act (PIPEDA), the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the United States (EU-U.S. Privacy Shield) – all of which allow personal data to flow safely from the EU to these countries.

Technology, Business Models and Personal Data Privacy and Protection

Data privacy and data protection are two separate but overlapping issues. Personal data can be abused in several ways; personal data can be misused, gathered or used without permission, it can be stolen (for sale or identify theft), or corrupted in the form of falsification. Personal data laws cover primarily the abuse of data, but this also likely requires additional reporting by a data controller. The process may also involve financial liability, where a data controller is found to be at fault through lax or negligent security arrangements.

Besides obligations on the data controllers, for the first time, the GDPR has also introduced direct obligations for data processors. Data processors are now also subjected to the penalties and civil claims by data subjects. The former directive only held data controllers liable for data protection noncompliance. GDPR states that, where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation, as well as ensure the protection of the rights of the data subject. While the onus remains on data controllers, i.e. customers of data processors, to only choose processors that comply with the GDPR, data processors too face direct obligations to comply with GDPR or face sanctions and potentially hefty fines. As supervisory authorities enforce penalties on controllers for a lack of proper vetting, processors may find themselves obligated to obtain independent compliance certifications to reassure their customers.[9]

But compliance with consent is problematic. When Facebook rolled out facial recognition tools in the EU, it promoted the technology as a means to help people safeguard their online identities. This was a risky move by the social network. Six years earlier, it had deactivated the technology in Europe after regulators there raised questions about its facial recognition consent system. Now, Facebook was reintroducing the service as part of an update of its user permission process in Europe.[10] Yet this could also be a huge reputational risk: aggressively pushing the technology at a time when its data-mining practices are under heightened scrutiny in the US and Europe. More than a dozen privacy and consumer groups, and at least a few officials, argue that the company's use of facial recognition has violated people's privacy by bypassing adequate user consent. Despite all of this, facial recognition technology is widely applied – enabled by ubiquitous cameras and increasingly accurate image analysis software. The technology has spurred conversations on one's privacy and growing worries that this technology could be used by governments to widely monitor people without their knowledge or consent.

How far other data privacy and data protection regimes, such as the provisions of the APEC CBPR and the country-specific personal data privacy and protection regulations across Asia-Pacific, are in compliance with GDPR are currently the foremost concern for companies trading with the EU. Mailboxes are already filling up with data policy statements sent out by enterprises, as customers

[9] https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/
[10] https://www.thestar.com.my/tech/tech-news/2018/04/28/what-facebooks-facial-recognition-feature-means-for-you/

start asking questions about what data is held about them, how is it used, what rights of sharing exist, etc.

> "With sweeping new rights for people to know how their data is being used, and to decide whether it is shared or deleted, business and regulators are being overwhelmed with complaints. Companies, which face fines of up to 4% of global turnover or €20m, whichever is greater, if they fall foul of GDPR, have reported a sharp increase in questions from customers." (*Financial Times*, 2nd July 2018)

Issues arising from GDPR can be summed around: complexity, compliance, and cross-border relations. Understanding the complexity of GDPR is a necessity to ensure compliance, without which cross-border data flows will be affected. This is especially true of services which often rely upon access to personal and sensitive data of customers based out of the EU; be it financial and payments data, household data or healthcare data.

The Implications

With increasing importance of data, classifying data according to how sensitive it is, who is considered the rightful owner of the data, the extent to which consent is deemed to have been given to collect and/or to share the data, who bears primary responsibility for the security of the data, how and where is the data stored, when should the data be destroyed, and so on, will be essential. In looking at each country's set of personal data privacy laws and regulations, these and other questions will arise. Whether by law or by enterprise decision, a Data Protection Officer (DPO) will become commonplace in the management of organisations collecting and/or processing large quantities of data. They will also become responsible for the translating of long obscure privacy policy statements into plain, simple, and concise language. Security-by-design will become a requirement, to either replace or improve legacy systems. There will also be a need for constant monitoring, testing, and upgrading of these systems in parallel with the growth of cyber-threats. Ultimately this needs to become the *de fault* practice of not only IT departments, but of all departments handling data, because security lapses can occur at any point along the chain of access. Once the new regulations and procedures have been completed, and the trial and error of cross-border trade has worked its way through the system – assuming GDPR is not dramatically revised under further legal challenge – it is anticipated that the focus will shift increasingly towards finding ways, using artificial intelligence (AI) for example, to monitor and neutralise cyberattacks, and maintain a steady and regular upgrading of security systems. There is also a possibility that this will be best achieved through a growing use of professional cloud services. For technology like blockchain (distributed digital ledgers) however, the primary security weakness remains in the points of user access to the cloud – for example, compromised nodes and devices – and in the communications between systems, which can be hacked.

In a world of AI and algorithms, data processing and monetisation has been accelerating rapidly. The impact of GDPR will be far reaching, and one area that will feel the effects sooner rather than later is AI. Organisations subject to the legislation will need to get explicit permission from users when they seek to collect, process, store, transfer, or otherwise use their data — and data is what AI needs to learn.

The Complexity: In brief, what is new about GDPR?

The GDPR consists of 99 Articles in 88 pages of text.[11] Following the European Court of Justice ruling, the Directive 95/46/EC was deemed as failing to meet the standards required of personal data privacy protection (para 9 below). The aims of the GDPR remain as they were under the Directive, to harmonise regulation across the EU, to assist the transfer of data for both commercial and personal reasons, while recognising that Member States have the right to different data classifications, such as local definitions of what constitutes 'sensitive' personal data (para 10 below). Thus, the complexity of GDPR is an effort to (i) fall within the law, (ii) harmonise across the EU, yet (iii) mirror the complexity across many different Member States. Paragraph 9 of the GDPR reads that while the objectives and principles of Directive 95/46/EC remain sound,

> it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC. [para 9]

And paragraph 10 affirms the rights of Member States to vary their personal data privacy regulations as the GDPR,

> provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful. [para 10]

Box 2: GDPR versus 1995 Data Protection Directive

GDPR differs from the Directive by introducing the following new provisions:[12]

- **Consent** must be requested in "an intelligible and easily accessible form" with reasons given
- **Data Subjects** have the right to receive in electronic form data held on them by data controllers or data processors on their behalf, described as "a dramatic shift to data transparency and empowerment of data subjects"
- **Right to be Forgotten**, or Right to Erase where data usage is complete, or consent is withdrawn, but subject to "the public interest in the availability of the data"
- **Data Portability** gives data subjects the right to share their data with other data controllers or migrate all of their data to a different data controller
- **Privacy by Design** requires data protection to be built into all new company data systems and not just added-on later
- **Data Protection Officers (DPOs)** are mandatory and strictly regulated appointments where the core business – regardless of its location – involves the personal data of residents of the EU

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[12] https://www.eugdpr.org/key-changes.html

- **Breaches** of GDPR are subject to a sliding scale of fines up to 4% annual turnover or €20 Million, whichever is greater.

Cost of Compliance

The GDPR threatens hefty fines for non-compliance, fines of up to 4% annual turnover or €20 million, whichever is greater, levied on businesses that fail to ensure adequate data protection or who hide data breaches or who collect and share information without permission. From the perspective of non-EU businesses trading with the EU however, there are two broader issues: (i) compliance that allows cross-border data flows in support of business activities which revolves around whether the personal data protection regime in a non-EU economy meets international standards (see below), and (ii) compliance with the terms of operation of GDPR with respect to the data chain involved in being an overseas data controller or data processor of data of EU citizens, or having a commercial agreement with an EU-based data controller or processor.

Businesses outside the EU trading with EU businesses or collecting data directly from EU residents – for example, e-commerce sites – need to adhere to the extra-territorial requirements. This includes the willingness and ability to provide digital copies of the data held on identifiable individuals upon request by the data subjects/owners; to take all the necessary steps to protect that data, to not share it without explicit consent, and to report serious breaches of data protection in a timely fashion. For example, a non-EU social media company that shares data with its app developers without the explicit permission of the data subjects, and the same app developer who subsequently misuses that data would both fall foul of the GDPR. Each business' data chain needs to start with consent from the data subject for the subsequent use of their data, and this should be done in a transparent manner. This can be problematic to establish and monitor, and there are many grey areas, such as visual and audio data that may get scooped up in a trolling exercise. Therefore, it is anticipated that regulatory and legal cases will arise within the EU if data subjects and interest groups make complaints of improper procedures or processes that threaten to jeopardise personal data privacy.

Consent - from the original OECD template,[13] the need to gain the consent of the data owner is a universal practice, except were public bodies are concerned. Currently APEC's CBPR excludes public bodies, while GDPR includes them. Within APEC itself, the practices differ: Hong Kong includes public bodies; Singapore excludes them; while in Thailand it remains unclear. GDPR goes further than CBPR by expressly requiring "explicit" consent for sensitive personal data, such as healthcare data. Several economies within APEC include provisions covering sensitive data and explicit consent, ranging from religion to sexuality, to political or trade union membership, and in some cases to financial assets, including Australia, Malaysia, the Philippines, South Korea, and Taiwan. For example, South Korea has recently allowed financial data deemed as sensitive to be stored in the cloud, but only within South Korea. Where explicit consent is unavailable, provision is usually made for data transfers that would benefit a person who lacks the capacity to give consent, such as medical data to an overseas clinic. Likewise, Thailand's PDPB also requires data controllers to obtain explicit consent from the data subject, either in writing or by electronic means prior to or at the time of data collection unless one of the prescribed exceptions applies.

More controversially, the GDPR raises questions over the collection of data indirectly from persons, notably from social media sources. When social media companies frequently offer access to their

[13] http://www.oecdprivacy.org/ and http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

applications only on condition that the user permits the app to farm names and addresses from their contact list, or from their picture gallery, there is a question mark over whose consent is being requested. Clearly not the contacts, who are unaware of the harvesting of their details, but nevertheless find themselves the target of advertisers. Prior to May 2015, Facebook had also allowed third-party apps to access the contact lists of the app's users.[14] The leverage involved is a geometric progression, a cumulative way for social media to acquire personal data. This is likely to remain a black hole in GDPR until tested in a court of law, but already some companies, such as Continental (Germany) are privately forbidding their employees to use social media apps, such as WhatsApp and Snapchat, on company phones.[15] Even before the GDPR came into force, in February 2018, a regional court in Berlin ruled that Facebook has illegally accessed personal data because its *de fault* settings were too obscure to constitute informed users.[16]

In a world in which data sources proliferate, and in which through triangulation and the use of AI, anonymity is rendered virtually meaningless, the issue of consent will forever be contentious. This is giving rise to debates as to how data privacy regulations should adapt. For example, a property rights approach referenced in July 2018 by Peter Harris, Australia's Productivity Commissioner,[17] suggests consumers should be regarded as sharing ownership of their data with data controllers with the right to veto how it is to be used, and a requirement of the data controller to be transparent about who the data is being shared with. How any benefits might be shared is not elaborated, nor exactly how granulated would be the disclosure of who's data is being shared with whom. It is an effort that proceeds on the assumption of common interests to encourage a wider use of data. For example, if the data is being shared not with advertisers but with app developers there could be benefits either in kind (use of the app) or in revenues (from ads or subscriptions to the app). The GDPR does not address this issue, but it does give the data owner the rights to: (i) know what data is held about them, (ii) receive a digital copy and the right to correct errors and the right to erase (under certain circumstances), (iii) the right to have the data transferred to another data controller of their choice, such as a bank, an insurance company, a utility, etc. – in July 2018 Facebook, Google, Microsoft, and Twitter agreed to make it easy for customers to transfer their data across applications.[18] To comply with these, data controllers will need to retain the data in a format (a standard) that can be transferred without loss. Beyond data collection and the increasingly problematic need for consent, however, lies the equally problematic need for security.

Data Protection – These days, most users are aware of the ubiquitous threat, and growing sophistication of cyberattacks. The more connected the world grows, the more vulnerable it is. The greater threat however is probably qualitative: what gets hacked and with what consequences? In this context, personal data is unlikely to be ranked at the same level as critical national infrastructure (CNI) – an exception might be the hacking of 160 million outpatient medical records in Singapore, including those of the Prime Minister[19] – yet access to personal data is one of the means of access to passwords and the CNI. On 10th July 2018, it was reported in a British newspaper that a mobile app had leaked the personal details of its users including addresses and roaming locations, of over 6,000 government security staff, dramatically described as "spies".[20] In April 2018, Thailand's second

[14] https://money.cnn.com/2018/07/10/technology/mailru-facebook-russia/index.html
[15] https://sg.news.yahoo.com/germanys-continental-bans-whatsapp-phones-085753894.html
[16] https://finance.yahoo.com/news/german-court-rules-facebook-personal-135203880.html
[17] http://www.pc.gov.au/news-media/speeches/data-protection
[18] https://www.zdnet.com/article/google-data-transfer-project-will-help-you-move-your-data-between-services/
[19] https://www.cbronline.com/news/singhealth-hacked-pm
[20] http://www.dailymail.co.uk/sciencetech/article-5932965/Shocking-security-lapse-running-app-Polar-exposes-locations-personnel-MI6-GCHQ.html

largest mobile operator, True Mobile was found to have suffered a data breach with the personal details of 45,000 customers data exposed – where both True Mobile and the discoverer of the leak had contrasting versions on how the data was breached/leaked.[21]

The first requirement of the GDPR is that companies whose primary business relies upon data collection appoint DPOs to manage, and avoid, exactly this type of situation. One of the responsibilities of the DPO under the GDPR is to ensure regular data processor audits and system reviews. Table 1 records that, besides the EU and in some cases in the US, in 14 Asia Pacific economies, five have provisions for DPOs.

Table 1 : Summary of Data Privacy Laws and Data Transfer Provisions

	Laws or regulations governing the collection, use or other processing of personal information	Effective agency (or regulator) tasked with the enforcement of privacy laws	Data controllers free from registration requirements	Cross-border transfers free from registration requirements	Breach notification law	Part of the APEC CBPR	Companies required to appoint 'Data Protection Officer'
Australia	Yes	Yes, NR	Yes	Partially	Partially	No	No
China	Partially	No	Partially	Partially	Partially	No	No
Hong Kong	Yes	Yes, NR	Yes	Partially	Partially	No	No
India	Partially	No	Yes	Yes	Yes	No	Yes
Indonesia	Partially	Yes, SR	Yes	Partially	Yes	No	No
Japan	Yes	Yes, NR	Yes	Partially	Partially	Yes	No
Malaysia	Yes	Yes, NR	Partially	Partially	No	No	No
New Zealand	Yes	Yes, NR	Yes	Partially	No	No	Yes
Philippines	Yes	Yes, NR	Partially	Partially	Yes	No	Yes
Singapore	Yes	Yes, NR	Yes	Partially	Partially	Yes	Yes
South Korea	Yes	Yes, SR	Yes	Yes	Yes	Yes	Yes
Taiwan	Yes	Yes, SR	Partially	Partially	Yes	No	No
Thailand	Partially	Yes, SR	Partially	Partially	No	No	No
Vietnam	Partially	No	Partially	Partially	No	No	No
EU	Yes	Yes, NR	Partially	Partially	Yes	No	Yes
USA	Yes	Yes, NR	Yes	Yes	Yes	Yes	Varies

NR = National Regulator, SR = Sectoral Regulator; updated from TRPC 2018[22]

The likelihood is that even where DPOs are not mandatory, more enterprises will choose to appoint them, partly to handle regulatory complexity, and largely to handle security. Article 25 of the GDPR requires "the principles of data protection by design and by default", in other words, security-by-design. And Article 42 calls upon Member States to establish "data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small, and medium-sized enterprises shall be taken into account."

[21] https://www.reuters.com/article/us-true-corporation-data/thai-telco-true-defends-security-measures-after-user-data-breach-idUSKBN1HO2D5

[22] http://trpc.biz/wp-content/uploads/APCC-ACCA_WhitePaper_CloudRegulations_2014_FullPaper.pdf

Security-by-design implies that upgrades bolted-on to legacy systems will not be easily accepted. The logic here is that cyberattacks can take place *anywhere* along the digital connectivity chain. If the lock of a door can be picked, or the bolts unscrewed, it matters not how thick is the door. Security is becoming a holistic issue, which means it is also becoming extremely difficult to monitor or pinpoint specific faults. An errant clerical worker, a senior manager, an outside contractor, are all equally capable of being hacked or phished. Even devices, systems, and apps with pre-installed malware are common tactics by professional criminals and state actors. In CNI enterprises, DPOs or their security officer equivalents, must be vigilant to detect and isolate any such device or app from use inside the premises. Personal data, although not usually part of the CNI, can be both a way into it, and a profitable source of access to intellectual property, firm secrets and ransomware, to bank accounts, credits cards and resale on the 'dark web'. Personal data privacy issues easily morph into national security issues. Data privacy and protection laws of a decade ago are thus often no longer fit for purpose.

There is a closing gap between cybersecurity for CNI and for the protection of data of all types. Given the universal nature of cyber threats, the GDPR's data-protection-by-design requirements of enterprises whose core business lies in data collection and data analytics will most likely become the *de facto* 'best practice' for the future.

Reporting – Under Article 56 of GDPR, notice of a data breach must be provided "without undue delay and, where feasible, not later than 72 hours after having become aware of it."[23] This would apply to a data breach anywhere along the data chain, from data controller to data processor, wherever they are located. Sanctions also apply to failure to delete data. In July 2018, Facebook was fined £500,000 by the UK's Information Commissioner's Office (ICO) after failing to ensure Cambridge Analytica – a company given access to personal data by Facebook and accused of the misuse of that data to assist a company campaigning for Brexit – had deleted the data.[24]

Data Deletion and Takedown – Deletion is becoming an issue as important as data harvesting. The "right-to-erase" or to be forgotten – but only under circumstances where a court of law may judge there is no public interest involved – is upheld by the GDPR. Outside of the immediate scope of the GDPR, but high in terms of public interest, is the deletion of content and/or bots that are considered illegal or subversive of the public good. For example, since May 2018, Twitter is reported to have deleted 70 million "fake or suspicious accounts."[25] Facebook however, has challenged a law approved by the German government in April 2018 that would fine a social media company up to €50 million (£43 million) for failing to takedown fake news or hate speech, on the grounds that it shifts the burden of judgement in cases that might be deemed free expression from the courts to the companies.[26] While there is nothing straightforward about these cases, they are subject to growing social and political concerns.

Cross-Border Data Flows

Cross-border data flows (CBDFs) is one area in which several APEC economies have made progress following the Cross-border Privacy Enforcement Arrangement (CPEA), which creates a framework for regional cooperation in the enforcement of Privacy Laws. Currently, seven APEC Economies are part of the CBPR: Canada, Japan, Mexico, United States, South Korea, the Philippines, and most recently

[23] https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/
[24] https://www.bbc.com/news/technology-44785151
[25] https://www.bbc.com/news/technology-44682354
[26] http://uk.businessinsider.com/facebook-says-germany-fake-news-plans-comply-with-eu-law-2017-5/?IR=T

Singapore,[27] with Australia planning to join soon.[28] In support of the CBPR, APEC ministers agreed "to protect the privacy of consumer data moving between APEC economies by requiring companies to develop their own internal business rules on cross-border data privacy procedures."[29] Compliance that allows cross-border data flows between the EU and non-EU jurisdictions revolves around three conditions.

- Local personal data protection laws and regulations must meet international levels.
- Data controllers and data processors must be accountable to their trading partners who are data controllers in the EU.
- Local data protection and security standards need to be convincing.

As Table 1 shows, most economies of the Asia-Pacific region have personal data protection laws that, at the most general level, would seem to comply with GDPR requirements. Perhaps more questionable is the third bullet point, the prevailing standards of security. The GDPR imposes requirements within the EU, such as data protection by design, and certification of data security systems, and these standards will need to be maintained whenever data is transferred out of the EU, but the adoption of data protection standards is far from universal.

In many of the APEC economies, international data protection standards are generally regarded as being met, and APEC has taken steps to institutionalise these for purposes of cross-border data flows, across other APEC economies, as well as with the EU. Joining the CBPR requires businesses to have their data protection systems certified by Accountability Agents – although the cost of doing so currently appears to be beyond the reach of SMEs who wish to trade – and the data protection regimes of economies involved must be judged by a Joint Oversight Panel as in harmony with the following principles:

- the effective protection of consumer personal information privacy in a system trusted by consumers;
- that implementation can be flexible enough to be adapted to the particular domestic legal environment of APEC Economies, while providing certainty for system participants;
- the regulatory burden on business is minimised while allowing business to develop and comply with effective and coherent rules for cross-border flows of personal information.

Box 3: APEC Cross-Border Privacy Rules (CBPR)

The CBPR was drafted based on the APEC Privacy Framework with priority on creating a 'global compliance system' by following nine of the APEC information Privacy Principles. These principles are: Preventing Harm, Notice, Collection Limitation, Use of Personal Information, Choice, Integrity of Personal Information, Security Safeguards, Access & Correction, and Accountability. The system was endorsed by APEC member economies in 2012 for businesses established in the APEC region that collect and transfer personally identifiable information from consumers. An important feature of the CBPR to note is that the system is an entirely voluntary one. Nations who wish to participate, are required to have an existing enacted privacy legislation. This was made as a pre-requisite because members are also required to map their local law to CBPR's framework as one of the steps during their application process.

[27] https://www.pdpc.gov.sg/pdpc/news/press-room/2018/03/singapore-joins-apec-cross-border-privacy-rules-and-privacy-recognition-for-processors-systems
[28] https://www.natlawreview.com/article/gdpr-looms-australia-to-participate-apec-s-cbpr-program
[29] https://www.apec.org/Press/Features/2013/0903_cbpr.aspx

Thailand's Personal Data Protection Bill

Thailand's Ministry of Digital Economy and Society (MDES)'s latest draft of the Personal Data Protection Bill (PDPB) was published for public consultation in September 2018 before a final revision is expected by the MDES and submission to the National Legislative Assembly (NLA) for approval.[30] The long awaited data protection law has been in the works since at least 2014, and was actually expected to have been passed earlier this year, exacerbated by the aforementioned True Mobile data breach.

The PDPB is one of six pending digital economy bills/amendments being proposed at the moment, and the PDPB plays the instrumental role in establishing a privacy framework and foundation for other digital economy plans. This includes the Digital Identification Bill, which also encompasses the formation of a National Digital Identification Company as the main operator to identify, authenticate citizen's digital IDs, and issue licences to identification providers.[31] The PDPB will ensure that personal data collected for digital IDs will be governed by safeguards on what data can be collected and used, and how consent is provided for.

Amendments made to the latest version of the draft PDPB include a shortened transition period for companies, definitions of personal data, extraterritorial applicability, data subject notification requirements, consent requirements, exemptions for collection of personal data from other sources, and explicit consent requirements for sensitive data. The amended draft of the PDPB also introduces the concept of exemption of explicit consent required from a data subject.[32] Out of these amendments, there are concepts adopted and introduced from the EU's GDPR.

Some examples include:

i) the data subject's right to data portability, the right to object, and the right to obtain a copy of the data undergoing processing;
ii) explicit consent of a data subject not required for collecting personal data if it is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract,[33]
iii) extraterritorial applicability, and
iv) the mandatory appointment of a representative for controllers or processors whose businesses are not based in Thailand.[34]

Unlike the GDPR however, which clearly defines the limits of penalties of up to 4% annual turnover or €20 million (whichever is greater), the limitations for violating the bill are not as clear, with the court empowered to levy punitive damages of up to twice actual charges.[35]

[30] https://www.lawplusltd.com/2018/09/draft-thailands-personal-data-protection-bill-open-public-hearing/
[31] https://www.biometricupdate.com/201809/thai-digital-identity-bill-faces-cybersecurity-and-privacy-scrutiny
[32] https://www.lawplusltd.com/Newsletter/Z004.0912.Updates%20on%20Personal%20Data%20Protection%20Bill.pdf?_t=1536833978
[33] https://www.lawplusltd.com/2018/09/draft-thailands-personal-data-protection-bill-open-public-hearing/
[34] https://www.aicasia.org/wp-content/uploads/2018/09/Submission-from-AIC-on-Thailand-PDPB-consultation-200918.pdf
[35] https://www.lawplusltd.com/2018/09/draft-thailands-personal-data-protection-bill-open-public-hearing/

Implications of the PDPB

The revised draft of the PDPB clearly indicates that the government has taken into consideration international regulatory frameworks, with particular focus on the GDPR, when formulating the detailed provisions with a view to achieve greater integration and harmonisation with global practices to reduce compliance costs for local businesses. For companies that already have a robust data protection regime in place and are already complying with GDPR, the changes required to accommodate the proposed PDPB will not likely to be substantial.

Organisations such as the Asia Internet Coalition caution that the adoption of a personal data protection framework that closely aligns with the GDPR may be premature in Thailand.[36] The cost of compliance to the PDPB will be prohibitively high for SMEs with provisions such as those that require organisations to notify or obtain approval from the enforcement authority of any cross-border data transfer. By imposing restrictions on cross-border personal data transfer without providing other accountability-based mechanisms, the PDPB will also impede technological innovation development. Unlike European nations, SMEs in Thailand will likely have had little prior experience complying with any form of privacy requirements with the PDPB being the first general privacy framework for the country.

With the extraterritorial reach of the PDPB, the applicability spectrum of the law will be widened to also cover organisations without a presence in Thailand but that process the data of individuals who reside in the country. Overseas organisations and enterprises that collect, process, and analyse data of Thai citizens may refrain from offering goods and services to data subjects in the country before they completely review and revise these processes for compliance. This will inevitably impact e-commerce and cross-border data flows. And while the EU can count on the mass of its economy to 'incentivise compliance', Thailand's economy is significantly smaller.

To provide sufficient time for data controllers and data processors to have the rigorous and necessary data protection measures in place and lessen the immediate impact of the PDPB to their business, the government should consider extending the transition period rather than shortening it from one year to 180 days and adopting a phased approach for provisions such as extraterritorial application to take effect. In particular, for SMEs, the government needs to not only provide a longer allowance for SMEs to achieve compliance, but also put in place supporting mechanisms and programmes to help them achieve compliance, as well as help them understand the importance in protecting user data and instilling trust in their services. The importance of building trust in today's digital world should not be underestimated. In a world where data has become the new economy, being able to demonstrate transparency, responsibility, and accountability will count for far more for a company than a prime-time commercial slot. Compliance can now be seen as a worthy investment as a business differentiator rather than additional costs or tick-box exercise.

Thailand currently is not a participatory economy of the APEC CBPR, and without a comprehensive legal framework on personal data protection, Thailand will not be able to join CBPR. The current draft of the PDPB has provisions on collection limitation, notice, and consent which are consistent with the principles set out in the APEC Privacy Framework and based upon OECD privacy guidelines. For example, the draft PDPB specifies that the collection of personal data must be for a lawful purpose and be directly relevant to, and necessary for, the activities of the data controller. Also, data subjects have the right to access their personal data and to request data controllers to disclose the

[36] https://www.aicasia.org/wp-content/uploads/2018/09/Submission-from-AIC-on-Thailand-PDPB-consultation-200918.pdf

sources of information. Thailand could thus potentially join the CBPR once it passes the PDPB. The enforcement of PDPB and the establishment of an independent national regulatory authority will represent one step forward for Thailand to participate in the CBPR system alongside other ASEAN countries like Singapore and the Philippines.

Thailand's belated PDPB puts it in a better position to enact a modern, forward-looking and future proof privacy framework as the foundation of Thailand's digital economy. By making a concerted effort to align with international frameworks such as the GDPR and APEC Privacy Framework, the PDPB not only refrains from reinventing the wheel, it makes regional and international compliance more straightforward. Likewise, when local companies will likely find it easier to expand overseas if the additional compliance costs are not too costly.

Moving forward however, the government needs to ensure adequate support is provided for many of the local SMES and manage expectations on the timeframe for compliance, where many SMEs will lack the necessary capacity and resource on how to comply with the PDPB.

Additional Resources

1) ASEAN ICT Masterplan 2020 – Framework on Personal Data Protection

2) GDPR Documents
    a. Regulation (EU) 2016/679 (General Data Protection Regulation)
    b. European Commission: Data Protection Page
    c. Information Commissioner's Office (ico) Guide to the General Data Protection Regulation (GDPR)

3) CBPR Documents http://www.cbprs.org/
    a. APEC: "Survey on the Readiness for Joining Cross Border Privacy Rules System Report – CBPRs"
    b. APEC Cross-border Privacy Enforcement Arrangement (CPEA) - creates a framework for regional cooperation in the enforcement of Privacy Laws

4) Thailand Law Amendment – Personal Information Protection Bill September 2018

5) Data Protection Knowledge Center

6) Graham Greenleaf and Arthit Suriyawongkul - Thailand's Draft Data Protection Bill: Many Strengths, Too Many Uncertainties