Balancing Privacy and Opportunity

in Hong Kong and the Asia Pacific Region

TRPC

Briefing Paper
13 December 2018

Table of Contents

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 in a more siloed manner, with more limited volume and scope. Sometimes retailers would gather personal data in pursuit of loyalty schemes, but few such instances had the objective of selling data to third parties. 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, location data and other information about their online habits – 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 the EU 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 controller, however under the GDPR, this now extends to include the entity, wherever located, if they are providing services to or monitoring individuals in the EU. This means that companies involved in the transfer of data from any resident of the EU, must not only operate in accordance with jurisdictions where they are located, but should also be compliant to the standards set by the GDPR. 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 Hong Kong-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. The Privacy Commissioner for Personal Data (PCPD) in Hong Kong provides guidance to local organizations on the issue, and suggests that "factors such as the use of a language or a currency of one or more member states in ordering goods and services, may make it apparent that the data controller

[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.pcpd.org.hk/english/data_privacy_law/eu/files/eugdpr_e.pdf

envisages or targets at offering goods or services to individuals in the EU, and hence be caught by the GDPR."[4]

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. The focus of personal data privacy policies 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, is ultimately judged by the European Court of Justice. For example, as demonstrated by the enhanced 'data protection by design' security provisions of the GDPR. 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 upon 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.[5] However, this arrangement is already being challenged by Max Schrems, a young Austrian lawyer, and other data rights groups.[6]

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[7] – 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.[8]

Most recently the EU signed an agreement with Japan that recognizes 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.[9] 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.

This is the first time that the EU and a third country from Asia Pacific have agreed on a reciprocal recognition of the adequate level of data protection. Currently, the EU has adopted only unilateral

[4] https://www.pcpd.org.hk/english/data_privacy_law/eu/files/eugdpr_e.pdf
[5] 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
[6] https://iapp.org/resources/article/a-brief-history-of-safe-harbor/
[7] https://en.wikipedia.org/wiki/PRISM_(surveillance_program)
[8] https://www.scmagazineuk.com/updated-safe-harbour-ruled-invalid-european-court-justice/article/1479260
[9] http://europa.edu/newsroom/rapid-failover/ip-18-4501_en.pdf

adequacy decisions with 12 other countries – namely, Andorra, Argentina, and Canadian organizations 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.

In other economies in Asia, regulatory frameworks around privacy remain fragmented with some emerging economies such as Thailand, Indonesia, and Vietnam still in the midst of enacting their respective privacy rules – with many taking reference and adopting concepts from the GDPR. The advantage for these economies is that they have an opportunity of enacting a forward-looking framework taking into account new technological risks, as well as align with international frameworks such as GDPR and CBPR.

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 EU Data Protection 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 less 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.[10]

But compliance via consent can be 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 has reintroduced the service as part of an update of its user permission process in Europe. 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.

[10] https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/

How far other data privacy and data protection regimes, such as the provisions of the APEC CBPR and the country-specific personal data privacy regulations across Asia-Pacific, are in compliance with GDPR is a concern for companies trading with the EU.[11] Mailboxes are already filling up with data policy statements sent out by enterprises, as customers start asking questions about what data is held about them, how it is 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 that 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

In looking at each country's personal data privacy laws and regulations a set of important standard questions arise: how do you classify data according to its sensitivity, what rights and responsibilities do different parties have in personal 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 and when should the data be destroyed. Whether by law or by enterprise decision, a Data Protection Officer (DPO) will become commonplace as organisations manage the collection and/or processing of increasingly large quantities of data. They will also become responsible for ensuring privacy policy statements are in plain, simple and concise language. Security-by-design will become a requirement. 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 implemented, 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 challenges – it is anticipated that the focus will shift increasingly towards finding ways, using AI for example, to monitor and neutralise cyber-attacks, 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. However, like blockchain technology (distributed digital ledgers), the primary security weakness will remain 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.

[11] https://legal.thomsonreuters.com/en/insights/articles/cost-of-compliance-2018-report-your-biggest-challenges-revealed

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

The GDPR consists of 99 Articles in 88 pages of text. [12] The aims of the GDPR remain as they were under the Directive, to harmonise data protection across the EU, to assist with the transfer of data for both commercial and personal reasons, while recognising that Member States have the right to exercise a number of derogations 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:[13]

- **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 in many instances where the core business – regardless of its location – involves the personal data of residents of the EU
- **Breach Notification** is a mandatory in many instances
- **Fines** are subject to a sliding scale of fines up to 4% annual turnover or €20 Million, whichever is greater.

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

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. However, from the perspective of non-EU businesses trading with the EU 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 requirement 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 a legitimate basis for the processing of their personal data, and this should be done in a transparent manner. However, 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,[14] the need to gain the consent of the data subject is a universal practice, except where 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. 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, 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.

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 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 also allowed third-party apps to access the contact lists of the app's users.[15] 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

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

[15] https://money.cnn.com/2018/07/10/technology/mailru-facebook-russia/index.html

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.[16] 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.[17]

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,[18] 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 directly, 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.[19] To comply with these, data controllers will need to retain the data in a format (a standard) that can be transferred without loss. However, beyond data collection and the increasingly problematic need for consent, lies the equally problematic need for security.

Data Protection – These days, users are increasingly aware of the ubiquitous threat, and growing sophistication of cyber-attacks. 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[20] – yet access to personal data is one of the means of access to passwords and the CNI. On 10 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".[21] The first requirement of the GDPR is that companies whose primary business relies upon data collection appoint Data Protection Officers (DPO) to manage, and help 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

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

	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 where DPOs are not mandatory, more enterprises will choose to appoint them, to handle regulatory complexity. This is evident in Thomson Reuter's Annual Cost of Compliance Survey, with 55% businesses in Asia indicating an expected larger compliance team, the highest globally.[23] 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."

Security-by-design implies that upgrades bolted-on to legacy systems will not be easily accepted. The logic here is that cyber-attacks 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 and their security officer equivalent, 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

[22] http://trpc.biz/wp-content/uploads/APCC-ACCA_WhitePaper_CloudRegulations_2014_FullPaper.pdf
[23] https://legal.thomsonreuters.com/en/insights/articles/cost-of-compliance-2018-report-your-biggest-challenges-revealed

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 cyber-security for CNI and for the protection of data of all types. Like GDPR and many national data protection laws, Singapore's Cybersecurity Act 2018 states that owners of CNI must "cause an audit of the compliance of the critical information infrastructure" every two years and "conduct a cybersecurity risk assessment of the critical information infrastructure" once a year.[24] 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."[25] 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.[26]

Data Deletion and Takedown – Deletion is becoming an issue as important as data harvesting. The "right-to-erase" or to be forgotten is upheld by the GDPR, where for examples, individuals have the right to have their personal data erased should they withdraw consent, or where the data collected is no longer necessary for the purpose to which it was originally collected. 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."[27] However, Facebook 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.[28]

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, namely Canada, Japan, Mexico, United States, South Korea, the Philippines, and most recently Singapore,[29] with Australia planning to join soon.[30] 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."[31] Compliance that

[24] https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312#pr15-
[25] https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/
[26] https://www.bbc.com/news/technology-44785151
[27] https://www.bbc.com/news/technology-44682354
[28] http://uk.businessinsider.com/facebook-says-germany-fake-news-plans-comply-with-eu-law-2017-5/?IR=T
[29] Personal Data Protection Commission Singapore (PDPC) (2018) Singapore joins APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems, https://www.pdpc.gov.sg/pdpc/news/press-room/2018/03/singapore-joins-apec-cross-border-privacy-rules-and-privacy-recognition-for-processors-systems
[30] The National Law Review (2018) As GDPR Looms, Australia to Participate in APEC's CBPR Program, https://www.natlawreview.com/article/gdpr-looms-australia-to-participate-apec-s-cbpr-program
[31] https://www.apec.org/Press/Features/2013/0903_cbpr.aspx

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 Asia -Pacific region have personal data protection laws that, at the most general level, would seem to comply with GDPR requirements, albeit to varying degrees. 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, 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. 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.

Combating Financial Crime

For financial institutions, complying with consent requirements and combating financial crime can appear to directly contradict – where on the one hand data privacy laws regulate and limit how, when and why personal data can be collected, processed and used, and on the other combating financial crime requires financial institutions to collect, process and analyse large volumes of personal data so as to identify and prevent money laundering and the committing of financial crimes. In an already highly regulated sector, a big question mark that arises from new compliance requirements within these data

laws are how does it affect the ability of financial institutions, regulators, and law enforcement agencies to combat financial crime?

Recognizing the importance of financial crime prevention, there are a number of exceptions within the GDPR that provide exemptions on financial crime prevention. Recital 47 of the GDPR clearly states that "the processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned". [32] Likewise, under Recital 71 "…decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes…".[33] To this extent some banks appear to have already been informing their clients that legitimate interests under the GDPR justifies their processing for anti-money laundering and anti-fraud.[34] The challenge then, is how to distinguish between normal data processing, and when data is being processed for financial crime prevention and thus further analysed – where the onus will be placed on financial institutions to document, assess and demonstrate legitimate interest.

The issue of balancing between stronger privacy safeguards from the GDPR, and ensuring financial prudence in combating financial crimes remains an important issue for a global financial centre such as Hong Kong, which process the data of over 10,000 finance-related firms, many with cross-border data flows.[35]

Data Futures

The issues outlined above are likely to become more, not less, complex as the role of data, the classifications of data, and definitions of data – data to a computer scientist, to a statistician and to a commercial enterprise can mean very different things – evolve and grow in industrial significance. Developments such as AI and the refinement of algorithms depend upon access to vast quantities of data and from a variety of sources ('Big Data') which often defy the premise of personal data privacy and ways must be found to accommodate privacy, innovation and public security. For example, it could be argued that social media companies and app promoters should be forbidden by law to request access to personal contact lists as these clearly violate the privacy of those on the list who are offered no chance to give consent and remain ignorant that their data may be being shared with organizations of which they disapprove. Currently they are only being pressured to give the immediate data subject the choice without losing access to the app. Another consideration is that culturally, attitudes to data access and sharing differ widely across societies.

GDPR includes the right of the data subject to request data portability. Australia has recently adopted this 'consumer right' as part of its Open banking initiative – following a report from the Productivity Commission – under which customers may ask their data to be shared with trusted third parties, for example, with different mortgage brokers to test the availability of costs of mortgages. [36] Innovations such as these are likely to be ongoing.

[32] http://www.privacy-regulation.eu/en/recital-47-GDPR.htm
[33] https://gdpr-info.eu/recitals/no-71/
[34] https://www.niceactimize.com/blog/Lawfulness-of-Financial-Crime-Data-Processing-under-GDPR-574
[35] https://www.statistics.gov.hk/pub/B71804FB2018XXXXB0100.pdf
[36] https://www.accc.gov.au/speech/consumer-data-and-regulatory-reform

Appendix

Table 2: CBPR vs GDPR[37]

	CBPR	GDPR
Purpose	To develop effective privacy protections that avoid barriers to information flows, and ensure continued trade, and economic growth in the APEC region.	To enable free movement of personal data within the Union while protecting fundamental rights and freedoms of natural persons and their right to the protection of personal data.
Material scope	Applies to persons or organizations in the public and private sectors who control the collection, holding, processing, use, transfer or disclosure of personal information.	Applies to the processing of personal data in the European Union.
Territorial scope	Applies to the same extent that the laws of each member country apply.	Applies to processing that takes place in the Union or by a processor who has an establishment in the European Union within the context of activities in the European Union or to processing activities that are related to the offering of goods and services to (or behavioural monitoring of) data subjects in the European Union.
Personal information	Personal information means any information about an identified or identifiable individual. (same)	Personal data means any information relating to an identified or identifiable natural person.
Data controller	Personal information controller means a person or organization who controls the collection, holding, processing or use of personal information.	Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processors	APEC Privacy Framework and CBPRs do not apply to processors, only controllers.	Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Publicly available information	The APEC Privacy Framework has limited application to publicly available information. Notice and choice requirements, in particular, often are superfluous where the information is already publicly available, and the personal information controller does not collect the information directly from the individual concerned.	The processing of publicly available information may be permitted for certain archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, insofar as providing notice is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the

37 https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/

		data subject's rights and freedoms and legitimate interests, including making the information publicly available.
Permitted member country variations (derogations)	Economies implementing the framework at a domestic level may adopt suitable exceptions to scope that suit their particular domestic circumstances. The framework is not intended to impede governmental activities authorized by law when taken to protect national security, public safety, national sovereignty or other public policy.	Member States have discretion in a number of subject areas including: Supervisory Authority; Sanctions; Demonstrating Compliance; Data Protection Officers; Archiving and Research; Third Country Transfers; Sensitive personal data and exceptions; Criminal Convictions; Rights and Remedies; Processing of Children's Personal Data by Online Services; Freedom of Expression in the Media; Processing of Data; Restrictions; Rules surrounding Churches and Religious Associations. Exceptions to general GDPR applicability also exist for national security, public safety, and police powers.
Preventing harm principle	Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information.	Protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
Notice	Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information. All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable. It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information. Where personal information is not obtained directly from the individual, but from a third party, it may not be practicable to give notice at or before the time of collection of the information.	If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. The processing of publicly available information may be permitted for certain archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, insofar as providing notice is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

Collection limitation	The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Use limitation	Personal information collected should be used only to fulfil the purposes of collection and other compatible or related purposes except: a) with the consent of the individual whose personal information is collected; b) when necessary to provide a service or product requested by the individual; or, c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Choice and consent	Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.	Permits the use of sensitive personal data with explicit consent from the subject, unless reliance on consent is prohibited by EU or member state law. "Explicit consent" must meet a higher standard than consent for the processing of other forms of personal data — an individual must be clearly informed of the use of their data and take an affirmative action to demonstrate their consent. Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Data integrity	Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.	Personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Security safeguards	Personal information controllers should protect personal information	Taking into account the state of the art, the costs of implementation and

	that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.	the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
Access and correction	Individuals should be able to obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them, and have access to information held about them, challenge the accuracy of information relating to them, have the information rectified, completed, amended or deleted. All of the above rights subject to a balancing of the burden or expense of compliance, legal or security reasons, the protection of commercial information, the protection of the privacy rights of persons other than the affected individual.	The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and to access to the personal data and information about the processing including: what categories of data are processed, the recipients of the data, and rights to erasure and rectification of the personal data, the right to lodge a complaint with a DPA, the source of the data, whether the data was subject to automated profiling (and if so, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject).
Accountability	A personal information controller should be accountable for complying with measures that give effect to the Principles stated above.	The controller shall be responsible for, and be able to demonstrate compliance with, the principles of the processing of personal data under the GDPR.
Transfer of personal data to another person or country	When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.	When a controller sends data to another party to be processed, they are a processor and therefore must be bound by contract with the controller to protect the personal data. Personal data may only be transferred to third countries where the EU has considered the laws to provide adequate protection or where protected by a binding corporate rules, approved model clauses, binding agreements combined with an approved code of conduct or approved certification.

Breach definition	There is no specified definition of breach under the APEC Privacy Framework or CBPRs.	Personal data breach means a breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Breach notification	The APEC Privacy Framework does not directly address breach, but the principles support notification. The CBPR to which APEC economies must bind themselves to join, require that member countries impose rules requiring that data controllers contractually protect data by requiring notification to themselves by data processors, agents, contractors or other service providers. The CBPRs do not require that member countries impose mandatory notification of breach to privacy enforcement authorities or data subjects.	The GDPR requires assessment of data incidents and prompt notification of breach to supervisory authorities and data subjects when there is a high risk to the rights and freedoms of natural persons and, with respect to supervisory authorities.
Breach mitigation	(see above) The APEC Privacy Framework requires that appropriate safeguards. The CBPRs require the applicant country to describe how it enforces a requirement to have technical (authentication and access control, encryption, firewalls and intrusion detection, audit logging, monitoring, etc.) and administrative (training, policies, enforcement, etc.) Safeguards.	Notification to data subjects is not required if: the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption; or the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialise. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Additional Resources

1) Privacy Tracker (iapp), Comparisons of GDPR & CBPR: https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/

2) Internet Commerce Australia: "Two approaches to Privacy – GDPR & CBPR" http://www.inca.com.au/news/blog/two-approaches-to-privacy-gdpr-cbpr.html

3) 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)

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

5) Privacy Commissioner for Personal Data, Hong Kong: EU General Data Protection Regulation (GDPR) , https://www.pcpd.org.hk/english/data_privacy_law/eu/eu.html

6) Thomson Reuters, Cost of Compliance 2018 Report, https://legal.thomsonreuters.com/en/insights/articles/cost-of-compliance-2018-report-your-biggest-challenges-revealed