nextrends Asia

Ideas & insights from the East

Data Privacy & Protection: fragmented attitudes and regulatory framework across the Asia-Pacific

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Embassy of Switzerland in Australia

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI

swissnex network

Introduction

Over the past two decades, the production of digital data has grown at an unprecedented rate. The International Data Corporation forecasts that by 2025, the total number of connected IoT devices alone will reach 41.6 billion and generate 79.4ZB of data[2]. The importance and scale of the flow and storage of data have thus become complex geopolitical, trade and security issues. The complexity in addressing data flows from a regulatory perspective is relative to the critical role data plays in today's society and economy. Regulatory frameworks for data privacy are critical to facilitate cross-border data flows around the world. Governments across the Asia-Pacific region have therefore developed and implemented national data privacy frameworks that can protect the data of their citizens, while also allowing data to flow across borders in ways that would support trade and innovation. These frameworks encourage a degree of convergence across the region, however the regional data privacy and protection regulatory landscape remain fragmented overall[3].

Data privacy and protection frameworks: regional overview

The data privacy landscape in the Asia-Pacific region has undergone a dramatic transformation in the past decade. While the laws in the region share the same data privacy and protection principles found in most privacy laws in the world, they also reflect the particular and diverse cultures and histories of the countries in the region. Australia, Japan, Korea and Singapore now have comprehensive privacy laws. India could follow shortly with its privacy law tabled at Parliament, while China's current regime still based on sectoral rather than omnibus privacy laws, is also evolving toward a comprehensive framework for individual data rights and protection.

Japan and Korea have each put in place comprehensive frameworks that rank arguably among the world's most advanced and mature models of data governance. Japan introduced its personal information protection law in 1988 based on the OECD's eight recommendation guidelines regarding data protection from 1980, but at the time, solely applicable to administrative organisations in the public sector. It then adopted the Act on the Protection of Personal Information (APPI) in 2003, expanding data protection requirements to private sector organisations, and becoming a pioneer for data protection legislation in Asia. This comprehensive law came into force in 2005 and was only

> The International Data Corporation forecasts that by 2025, the total number of connected IoT devices alone will reach 41.6 billion and generate 79.4ZB of data.

[1] This report focuses on China, Japan, India, Korea, Singapore and Australia where the swissnex network is represented.
[2] https://www.zdnet.com/article/iot-devices-to-generate-79-4zb-of-data-in-2025-says-idc/
[3] https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf

significantly strengthened in 2017 with new guidelines for the protection and appropriate handling of personal information following the establishment of an independent agency, the Personal Information Protection Commission (PPC). This amendment widened the scope of the APPI to all businesses in Japan regardless of the company's size. At the moment, only a few ministries and agencies still issue non-binding guidelines on the interpretation of the APPI for their respective sectors.

South Korea's comprehensive Personal Information Protection Act (PIPA), enacted in 2011, is one of the world's strictest privacy regimes. Like the EU's General Data Protection Regulation (GDPR), it protects privacy rights from the perspective of the data subject and it is comprehensive, applying to most organisations, even government entities, and strict with penalties including criminal and regulatory fines and even imprisonment[4]. In February 2020, South Korea merged the Personal Information Protection Law, the Law on the Use and Protection of Credit Information and other relevant sectoral regulations into PIPA. Subsequently, in March 2020, it amended the Personal Information Protection Law again on pseudonym processing, the institutional setting of the Personal Information Protection Commission, personal information processing of information and communication service providers among others. In January 2021, the Personal Information Protection Committee released the draft of new amendments to PIPA including the self-regulation mechanism, the introduction of the right to data portability for data subjects, clarifications on the regulation of use and processing of personal data during offline activities, and cross-border data transfers[5].

The Personal Data Protection Act 2012 (PDPA) is the principal data protection legislation in Singapore[6]. It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes. The PDPA was passed by the Parliament of Singapore in 2012 and took effect in phases starting with the provisions relating to the formation of the Personal Data Protection Commission (PDPC). The PDPC is the authority that administers and enforces the PDPA. The PDPA covers personal data stored in electronic and non-electronic forms. It takes into account the concepts of consent, purpose and reasonableness. The PDPA is meant as a baseline standard of protection for personal data across the economy and complement sector-specific legislative and regulatory frameworks. This means that organisations have to comply with the PDPA as well as the common law and other relevant laws that apply to their industry, when handling personal data in their possession. The PDPA generally applies to all organisations with respect to the personal data they collect, use and/or disclose with some exemptions (e.g. individuals acting in a personal or domestic capacity and public agencies or organisations acting on behalf of another public agency).

South Korea's comprehensive Personal Information Protection Act (PIPA), enacted in 2011, is one of the world's strictest privacy regimes.

[1] This report focuses on China, Japan, India, Korea, Singapore and Australia where the swissnex network is represented.
[2] https://www.zdnet.com/article/iot-devices-to-generate-79-4zb-of-data-in-2025-says-idc/
[3] https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf

Australia regulates data privacy and protection through a mix of federal, as well as state and territory laws. The Federal Privacy Act 1988[7] and its 13 Australian Privacy Principles[8] (APPs) govern standards, rights and obligations around: the collection, use and disclosure of personal information; an organisation or agency's governance and accountability; integrity and correction of personal information; and the rights of individuals to access their personal information. The APPs are principles-based law and technology neutral, which make them flexible and adaptable[9]. Most states and territories in Australia also have their own data protection legislation[10]. Additional parts of state and federal legislation relate to data protection for specific types of data or specific activities such as the Telecommunications Act 1997 (Cth) or the National Health Act 1953 (Cth). The government is currently reviewing Australia's Privacy Act and working on a separate track to increase the maximum civil penalties under the Act, and to develop a binding privacy code for social media platforms and other online platforms that trade in personal information. The "Assistance and Access Act" (AAA) provides law enforcement agencies with access to encrypted data for serious crime investigation. The legislation may have a much broader remit with limited judicial oversight and has been the subject of much criticism from local and global technology firms[11], as well as human rights and privacy defenders[12], who respectively fear that the legislation has the potential to significantly impact security and encryption solutions providers in Australia while also affecting individual human rights to privacy and freedom of expression, among others.

China's data privacy legislation is a mix of regulations and non-legally binding guidelines. The Cyber Security Law (CSL) was published in 2017. The law establishes basic privacy requirements but does not specify what exactly companies need to do to comply with key requirements regarding consent, anonymisation, and securing personal information. In 2018, the "Personal Information Security Specification" was released to provide detailed guidance for compliance in the processing of information (the collection, storage, use, sharing, transfer, and disclosure of personal information). In 2019, China's new e-commerce law took effect. It regulates e-commerce business operators that collect and use personal information. China's Data Security Law is still in drafting while the Personal Information Protection Law draft was released on 21 October 2020 for public consultation. Together with the cybersecurity law and relevant parts of the 2018 e-commerce law, China's Personal Data Protection Law will lead to

Australia regulates data privacy and protection through a mix of federal, as well as state and territory laws.

[4] https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/
[5] https://www.lexology.com/library/detail.aspx?g=c1a6c048-cb0a-4faa-8310-b02d36bce236
[6] https://platform.dataguidance.com/legal-research/personal-data-protection-act-2012-no-26-2012
[7] https://www.oaic.gov.au/privacy/the-privacy-act/
[8] https://www.oaic.gov.au/privacy/australian-privacy-principles/
[9] https://www.oaic.gov.au/privacy/australian-privacy-principles/
[10] These acts include: Information Privacy Act 2014 (Australian Capital Territory), Information Act 2002 (Northern Territory), Privacy and Personal Information Protection Act 1998 (New South Wales), Information Privacy Act 2009 (Queensland), Personal Information Protection Act 2004 (Tasmania), and Privacy and Data Protection Act 2014 (Victoria)
[11] https://www.afr.com/technology/time-for-industry-to-speak-up-on-australia-s-encryption-legislation-20191017-p531qq
[12] http://cdn.computerworld.com.au/article/647615/rights-groups-and-tech-giants-form-alliance-to-fight-encryption-bill/

a comprehensive framework for individual data rights and protection. India's proposed Personal Data Protection Bill, currently tabled in Parliament, lays down rules related to the transfer of personal data outside India[13]. It sets rules for how personal data should be processed and stored, and lists people's rights with respect to their personal information. It also proposes to create an independent new Indian regulatory authority, the Data Protection Authority, to carry out this law. The bill stipulates that all sensitive personal data are stored in India and that the most critical ones cannot be transferred out of India. The Bill also introduces stringent requirements related to mandatory data breach notification, consent to be obtained prior to collection and individual privacy rights. Presently, the Information Technology Act 2000 governs the protection of personal information, specifically electronic data and transactions.

The 'datafication' of society also reveals geopolitical stakes: in a world increasingly determined by data, political aspirations to regulate data flows are rarely neutral.

Data localization and sovereignty trends: India and China

The 'datafication' of society also reveals geopolitical stakes: in a world increasingly determined by data, political aspirations to regulate data flows are rarely neutral[14]. This evolution has transformed the relations between individuals and states. Furthermore, private companies have gained an immense control over data as a result of the digitalisation of the economy. As data collecting, processing and analysing agents, they now occupy a strategic and influential position in world affairs. These new dynamics have led states like China and India to explore new forms of territorial authority and pursue data sovereignty in a context where data is viewed as a new national resource.

China's Cyber Security Law requires operators of critical infrastructure to store domestically both personal information and data of Chinese citizens collected and produced in the course of their business operations. Many international companies have thus chosen to either hire local data server providers to migrate their data or build their own data centers. Apple is setting up a new data center in Guizhou and in partnership with local data management firm Guizhou-Cloud Big Data Industry (GCDB), a state-owned enterprise. In 2019, the Cyberspace Administration of China (CAC) issued draft measures on *Security Assessment on Cross-border Transfer* of Personal Information. The measures require all network operator's cross-border transfer of personal data to go through a security assessment to be conducted by a provincial branch of CAC. The cross-border transfer of personal data is prohibited if data transfer is

[13] https://www.prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf
[14] http://www.jstor.org/stable/23526834

likely to impact national security or public interest or impact the effective protection of personal data.

Under India's proposed Personal Data Protection Bill, the data localisation requirements and extraterritorial provisions exceed those found in the GDPR. The law would require businesses to store data on servers within the country while restricting cross-border transfers. It is also striking that the legislation grants the authorities the possibility to exempt itself from its requirements as well as the right to access business intelligence and intellectual property of companies for its own 'planning' and 'development' purposes[15,16]. The restrictive approach to data localisation has also extended to specific sectors. For instance, in 2018, the Reserve Bank of India issued directives to digital companies to store payments system related data in India. Several sectoral notifications mandating data localisation have been issued since.

The objectives of these provisions include aiding the protection of national interests and security, access to data for the purpose of investigation by law enforcement agencies, development of domestic tech companies, prevention of 'data colonialism' and taxation of digital companies (there is a view that jurisdiction control over data would act as a leverage for the government to collect taxes). The rules have significance for global as well as Indian tech companies, and have added to the complexity as well as their costs of doing business in India. New Delhi has been batting for its 'data sovereignty' vision at international fora. During the G20 summit in June 2019, India boycotted the Osaka Track for reasons that included the fact that it would have undermined the country's data localisation rules.[17] At the same time, it is reported that after initial resistance during the RCEP negotiations, India allowed for the e-commerce chapter to go ahead with provisions for free flow of data across borders[18].

Data privacy and protection discussions are gaining traction not only at the national level, but also within regional fora, and countries in the region have a long history of collaboration on digital governance and privacy

Convergence within the region

Data privacy and protection discussions are gaining traction not only at the national level, but also within regional fora, and countries in the region have a long history of collaboration on digital governance and privacy. One of the earliest initiatives was the establishment of the Asia-Pacific Telecommunity (APT) in 1979 on the joint initiatives of the United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) and the International Telecommunication Union (ITU). APT was set up as an inter-governmental organisation, focused on the region's telecommunication and ICT sectors. It has

[15] https://www.cov.com/-/media/files/corporate/publications/file_repository/comparison-chart--gdpr-vs-india-pdpb-2019-feb-03-2020.pdf
[16] https://www.mofo.com/resources/insights/210104-transformation-privacy-landscape-asia.html#_ftnref1
[17] https://dig.watch/updates/g20-osaka-track-raises-controversy
[18] https://www.thehindubusinessline.com/opinion/indias-irresponsible-flip-flops-at-rcep/article29924193.ece

38 members, including Australia, China, India, Japan, Korea and Singapore[19].

The Asia-Pacific Economic Cooperation (APEC) has also facilitated dialogue on data privacy and protection over the years. APEC is an inter-governmental forum that promotes free trade throughout the Asia-Pacific region. Its members include all the countries studied in this report with the exception of India. It developed the APEC Privacy Framework, a set of information privacy principles and implementation guidelines that reaffirm the value of individual privacy and the importance of information flow, while promoting e-commerce throughout the APAC region. The Framework forms the basis for a regional system called the APEC Cross-Border Privacy Rules (CBPR) that seeks to ensure the continued free flow of personal information across borders, while establishing a voluntary accountability mechanism for meaningful protection for the privacy and security of personal information. Australia, Japan, Korea and Singapore participate in the CBPR. The APEC Privacy Framework is important in Asia because it was the first framework developed specifically by and for Asian countries and their counterparts in the Americas (Canada, Mexico, and the United States). It incorporates a set of implementing measures to operationalise and enhance accountability[20].

Data privacy and protection regulations have also been included in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and in the Regional Comprehensive Economic Partnership (RCEP) under the respective e-commerce articles. Australia, Japan and Singapore participate in the CPTPP and thus endorsed its regulations on cross border data flow which stipulates, for instance, that no country can require a covered person to use or locate its computing facility, including its servers, in that country's territory as a condition for doing business there, thus constraining data localisation aspirations. Australia, China, Japan, Korea and Singapore (through the ASEAN) participate in the RCEP, a free trade agreement that, when ratified, will come to represent 30% of the world's GDP and population. RCEP aims to foster the movement of data and information across borders and digital trade. The cross-border data flows and localisation articles in RCEP are the first commitments of this kind for most of the signatories, yet they also leave the regulatory door ajar for each country to force hard, localisation rules for data without being subject to scrutiny at the multilateral platform[21].

With the notable exception of India, the countries studied in this report have all endorsed the 'Osaka Declaration of Digital Economy' at the G20 Summit in Osaka in 2019. The 'Osaka Track' is an overarching framework that promotes cross border data flow with increased protections and recognises data as an 'important source of economic growth'. Promoted by former Prime Minister of Japan, Shinzo Abe, it underscores the importance of 'Data Free Flow with Trust' (DFFT), a concept that calls for a set of international rules that will facilitate

The cross-border data flows and localisation articles in RCEP are the first commitments of this kind for most of the signatories, yet they also leave the regulatory door ajar for each country to force hard, localisation rules for data without being subject to scrutiny at the multilateral platform"

[19] https://www.mondaq.com/india/data-protection/958700/introduction-to-digital-governance-issues-in-the-apac-region-

[20] https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf

[21] https://www.cigionline.org/articles/digital-trade-rcep-wtos-future

e-commerce as well as free cross-border movement of data, and remove restrictions on data storage in foreign servers[22].

On the bilateral level, Singapore has been pioneering digital economy agreements with countries in the Asia-Pacific region (Australia, Chile and New Zealand). Singapore and the Republic of Korea have also launched negotiations on a new Korea-Singapore Digital Partnership Agreement (KSDPA). The agreement seeks to deepen bilateral cooperation in new emerging digital areas, such as in personal data protection and cross-border data flows, digital identities, fintech, as well as Artificial Intelligence governance frameworks.

On the bilateral level, Singapore has been pioneering digital economy agreements with countries in the Asia-Pacific region

…and beyond: global standards

The European Union (EU) and Japan have been having dialogues on the transfer of personal data since April 2016. In the joint statement of Japan's PPC and EU's Directorate-General for Justice and Consumers of 17 July 2018, both parties announced mutual recognition of each other's personal data protection systems. The decision was reached two months after the General Data Protection Regulation (GDPR) came into effect and strengthened strategic partnerships as well as the bilateral Economic Partnership Agreement. For the EU, it was the first agreement based on mutual recognition of adequate data protection with a third country. Adequacy talks are ongoing between the EU and South Korea[23].

[22] https://www.mondaq.com/india/data-protection/958700/introduction-to-digital-governance-issues-in-the-apac-region-#_ftn14
[23] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Conclusion

The countries studied in this report are strengthening their data privacy and protection laws. The different models developed often reflect the culture they emanate from, as well as the region's heterogeneity: innovative cross-border data flow governance models contrast starkly with data localisation models. The opportunities associated with the digital economy are indisputable and digital trade is therefore an evolving area of friction. In the Asia-Pacific region, an ongoing economic integration is on the way on both bilateral and multilateral levels and illustrate the region's dynamism and importance as a critical link in the global digital economy and value chain.

nextrends Asia
Ideas & insights from the East