Deloitte.

1st EDITION

The Asia Pacific Data Localisation Guide 2023

Contents

Introduction

In our increasingly digital world, data localisation is an important tool for protecting user privacy and securing data. In essence, data localisation is the process of storing or processing data within the borders of a nation where the data is generated. According to an OECD paper, data localisation refers to the mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction.[1] While there is no singular definition of data localisation, data localisation usually comprises requirements for the physical storage of data within defined physical boundaries. It also includes measures that help ensure the safe transfer of data across borders. These measures include the requirement to obtain consent (individuals, or regulatory bodies) before making the transfer, storage of a local copy of the data, and imposing taxes on data exports.[2]

History of data localisation

As the world moves toward a globalised existence, a need has been felt by many nations to re-assert their sovereignty. An increasingly common way of doing so is by exerting 'data sovereignty'. The practice of data sovereignty is a channel for governments to claim sovereignty over their citizens' data no matter where, or by whom, it is stored.[3] In 2005, the first steps to introduce data localisation were taken when the Government of Kazakhstan passed a law for all ".kz" domains to be run domestically (with later exceptions for Google). Post the Edward Snowden revelation of the United States Counter-Terrorism Surveillance Program, many others have tried to enact strict policies to be able to control the flow of residents' data through technology.[4]

Importance of data localisation

Data localisation aims to increase control over citizens' data by bringing decision making and access rights within jurisdictional boundaries.[5] The increased number of data localisation policies reflects the fear that nations have of losing or diluting their data sovereignty. Various regulations have been put in place for regulating the data flow across borders, with penalties defined for non-compliance.[6]

For developing nations, storing data locally can create an information asymmetry, allowing local companies to get a competitive edge and become more profitable than their non-local counterparts. Data storage in local data centres can give local companies and government easy access to the data, and local authorities are typically not required to invest into extra measures for enabling data accessibility as per legal requirements.

Nevertheless, localised data can help provide better visibility of the security measures in place, assuring individuals of protection and security of their data.

1. Dan Svantesson, "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines," *OECD Digital Economy Papers* No. 301, December 22, 2020. https://www.oecd-ilibrary.org/docserver/7fbaed62-en.pdf?expires=1659434582&id=id&accname=guest&checksum=E48A3C995857B5B56CA9195D22C6CA96
2. Rishab Bailey and Smriti Parsheera, "Data localisation in India: Questioning the means and ends," *NIPFP Working paper series*, October 31, 2018. https://www.nipfp.org.in/media/medialibrary/2018/10/WP_2018_242.pdf
3. *Ibid.*
4. Anirudh Burman and Upasana Sharma, *How Would Data Localisation Benefit India?*, Carnegie Endowment for International Peace, April 1, 2021. https://www.jstor.org/stable/resrep31117.4?seq=2#metadata_info_tab_contents
5. *Ibid.*
6. https://blog.ipleaders.in/significance-data-localisation-developing-countries/ and https://magehost.pro/en/data-localisation-the-pros-and-cons/

Introducing this guide

In the wake of data sovereignty and the rise in data localisation regulations across the world, this comprehensive guide was compiled to help identify data localisation requirements within the Asia Pacific region and the appropriate measures for protection of data in cross-border transfers.

Given the ongoing challenges of the need for data sovereignty and need to control data flow, we felt it important to provide a guide of regulations to assist businesses and compliance specialists with a general understanding of the nuances of the data localisation requirements across the Asia Pacific region.

This guide aims to showcase specific privacy and data localisation laws, regulations, and amendments currently in place and enforced in various parts of the Asia Pacific region. Official resource links that may be referred to for substantiating and implementing these legal requirements are also provided.

Manish Sehgal
Asia Pacific Cyber Data & Privacy leader

Ian Blatchford
Asia Pacific Cyber leader

Note: *This guide is not intended to be a complete legal reference and should not be solely relied upon for that purpose. We trust you will find the guide useful. However, we encourage you to consult a specialist for details regarding the legal requirements and steps of compliance. All information presented in this Guide is accurate and up to date as of 1 August 2022.*

Data localisation guides for Asia Pacific

Updates for data localisation requirements for the Asia Pacific region have been detailed in the following sections.

Australia

In Australia, data localisation requirements are found in various sectors such as data protection, health care, and finance.

Requirements endorsed by the applicable laws must be complied with for international data transfers and data storage requirements. These laws cover a wide range of information which includes personal data, financial data, health data and so on.

Disclaimer: This guide focuses on the federal laws of Australia and only a few sample state laws have been considered.

Applicable regulations

Privacy Act 1988 (Cth) (Law):

1. Australian Privacy Principle (APP) 8 of the Privacy Act 1988 (Cth) (Law):[7]

Applicability:
This Act protects the information of individuals who are "natural persons". This Act applies to all APP entities (agencies and organisations) and extends to all of Australia's external territories as well as to agencies or organisations outside Australia that have an Australian link.

Requirements:
This Act is regulated by the **Office of the Australian Information Commissioner (OAIC)** and came into force in 1989. The Act states that personal data about an individual can be disclosed to an overseas recipient only if a law/binding scheme is present that is similar to the APPs, the individual has given their consent, an Australian law/court order requires it, a permitted general situation exists, the disclosure is required by an international agreement or if an agency believes such disclosure is required for activities conducted by an enforcement body or if the recipient is an enforcement body.

Type of data:
This is applicable to personal data of individuals

Penalties:
Not applicable

Exemptions:
Not applicable

7. https://www.legislation.gov.au/Details/C2021C00452

2. Section 21D of the Privacy Act 1988 (Cth) (Law):[8]

Applicability:
This section of the Act is applicable to a credit reporting body in relation to their credit reporting information (including de-identified information), credit provider derived information and information collected via a pre-screening assessment. It is also applicable to credit providers in relation to their credit information, credit eligibility information and credit reporting body derived information.

Requirements:
This Act is regulated by the **Office of the Australian Information Commissioner (OAIC)** and came into force in 1989. It states that a credit provider must not disclose credit information about an individual to a credit reporting body (whether or not the body's credit reporting business is carried on in Australia) unless the credit provider is a member of or is subject to a recognised dispute resolution scheme, knows/believes on reasonable grounds that the individual is at least 18 years old, and the credit reporting body is an organisation with an Australian link. Further, the credit information that is transferred must not be related to any act, omission or matter that took place before the individual turned 18 and any consumer or commercial credit information that is transferred must be provided or applied for within Australia.

If any information being transferred is related to the repayment history of an individual, the credit provider transferring it must be a prescribed licensee, the consumer credit to which the information relates is consumer credit that has already been disclosed to the credit reporting body and the credit provider has complied with all the requirements related to disclosure under this regulation.

If the information being transferred is the default information of an individual, it must be ensured that the credit provider has sent a notice to the individual about disclosing the information to a credit reporting body and 14 days have passed since the notice was sent.

The credit provider must make a written note of all disclosures made to credit reporting bodies.

Type of data:
This section of the Act applies to credit related information of individuals

Penalties:
If this section of the Act is breached, a civil penalty of 2,000 units will be imposed

Exemptions:
Not applicable

8. https://www.legislation.gov.au/Details/C2021C00452

My Health Records Act 2012 (Law):[9]

Applicability:
This Act establishes the role and functions of a system operator, a registration framework for individuals and entities such as healthcare provider organisations, and a privacy framework that specifies which entities can collect, use, and disclose certain information in the My Health Record System.

Requirements:
This Act is regulated by the **Office of the Australian Information Commissioner (OAIC)** and came into force in 2012. It states that a system operator, registered repository operator, portal operator, or contracted service provider that holds records for the purposes of this Act must not hold/take records, process/handle information relating to records, or cause or permit another person to do so outside the territory of Australia.

However, the system operator can hold, take, process, and handle such information outside Australia that does not include personal information related to a healthcare recipient or participant in the My Health Record System or identifying information of an individual or entity.

Type of data:
This is applicable to personal data and health data of individuals

Penalties:
1. Any unauthorised collection, use or disclosure of health information in a My Health Record would result in the following:
   i. Civil Penalty – 1,500 penalty units (up to 7,500 penalty units for bodies corporate)
   ii. Criminal Penalty – 5 years imprisonment and/or 300 penalty units (up to 1,500 penalty units for bodies corporate)
2. Failing to notify an actual or potential data breach in which a person was directly involved would result in a civil penalty of up to 1,500 penalty units (up to 7,500 penalty units for bodies corporate).

Exemptions:
Not applicable

9. https://www.legislation.gov.au/Details/C2021C00475

Foreign Acquisitions and Takeovers Act 1975 (Law):[10]

Applicability:
This Act applies to all individuals (whether or not residents of Australia or Australian citizens), all corporations (whether or not formed or carrying on business in Australia) and all unit trusts (whether or not Australian trusts). This Act applies within and outside Australia.

Requirements:
The Act is regulated by the **Foreign Investment Review Board of Australia** and came into force in 2021. The Act empowers the Treasurer to prohibit or impose conditions on investment proposals made by foreign persons to acquire, or to increase, a substantial shareholding in, or acquire a controlling interest in, the assets of a prescribed Australian corporation valued above the relevant thresholds if they are contrary to the national interest of Australia. The Treasurer has the power to determine what will be classified as 'national interest' on a case-by-case basis as it has not been defined in the legislation.

The Treasurer may employ the following conditions for the treatment of sensitive data for approving a foreign investment proposal:

1. Developing and implementing data security policies and procedures that include requirements beyond the Australian Privacy Act
2. Only giving restricted access to directors, employees, and staff of the foreign investor
3. Imposing restrictions on the location of data storage and access
4. Ensuring that the foreign investor has implemented adequate cybersecurity procedure and reporting requirements in the event of a data breach.

Type of data:
This is applicable to sensitive data

Penalties:
It is a criminal offence to proceed with a foreign investment proposal without the approval of the Treasurer. The penalty imposed currently is $222 per unit.

Exemptions:
Not applicable

Health Records and Information Privacy Act 2002 (New South Wales [NSW]) (Law):[11]

Applicability:
Schedule 1 of this Act contains 15 Health Privacy Principles that govern how public and private sector organisations in New South Wales handle health information.

Requirements:
This Act is regulated by the **Information and Privacy Commission of New South Wales** and came into force in 2004. It mandates that an organisation can transfer the health data of individuals outside the jurisdiction of New South Wales only if a law/binding scheme similar to the law of NSW is in place, the individual has given their consent, the transfer is necessary for the performance of a contract between the organisation and the individual or between the organisation and third party for the benefit of the individual, the transfer is required under any other law, the organisation has ensured that the health data that is transferred will not be used inconsistently with the Health Privacy Principles, or the transfer is for the benefit of the individual and it would be reasonably impractical to obtain the individual's consent for the transfer.

Type of data:
This Act applies to health data of individuals

Penalties:
Not applicable

Exemptions:
Not applicable

10. https://firb.gov.au/guidance-notes
11. https://legislation.nsw.gov.au/view/html/inforce/current/act-2002-071#frnt-lt

Health Records Act 2001 (Victoria) (Law):[12]

Applicability:
This Act sets outs 11 Health Privacy Principles, which are contained in Schedule 1 of the Act. These principles outline how Victorian public and private sector organisations must handle health information.

Requirements:
This Act is regulated by the **Office of the Health Complaints Commissioner** and came into force in 2002. It mandates that an organisation can transfer the health data of individuals outside the jurisdiction of Victoria only if a law/binding scheme similar to the law of Victoria is in place, the individual has given their consent, the transfer is necessary for the performance of a contract between the organisation and individual or between the organisation and third party for the benefit of the individual, the transfer is required under any other law, the organisation has ensured that the health data that is transferred will not be used inconsistently with the Health Privacy Principles, or the transfer is for the benefit of the individual and it would be reasonably impractical to obtain the individual's consent for the transfer.

The transfer can also take place if it is necessary to lessen or prevent the following:

1. A serious and imminent threat to the life, health, or safety of the individual or another person, or
2. A serious threat to public health or public safety.

Type of data:
This Act applies to health data of individuals

Penalties:
Not applicable

Exemptions:
Not applicable

Privacy and Data Protection Act 2014 (Victoria) (Law):[13]

Applicability:
This Act is applicable to all organisations within Victoria that are transferring the personal data of individuals outside of Victoria.

Requirements:
This Act is regulated by the **Office of the Victorian Information Commissioner** and came into force in 2014. It mandates that an organisation can transfer the personal data of individuals outside the jurisdiction of Victoria only if a law/binding scheme/contract similar to the law of Victoria is in place, the individual has given their consent, the transfer is necessary for the performance of a contract between the organisation and an individual, it is for the implementation of pre-contractual measures taken in response to the individual's request or for the performance of a contract between the organisation and a third party for the benefit of the individual, the organisation has ensured that the personal data that is transferred will not be used inconsistently with the Information Privacy Principles under this Act, or the transfer is for the benefit of the individual and it would be reasonably impractical to obtain the individual's consent for the transfer.

Type of data:
This Act applies to personal data of individuals

Penalties:
Not applicable

Exemptions:
The following exemptions are applicable:

1. Any other laws (including Commonwealth laws) that require transborder flows will override the requirements of this Act
2. If the police reasonably believe that it is necessary not to comply with the requirements of cross-border transfers for law enforcement activities; or
3. If any court or tribunal, while carrying out their judicial or quasi-judicial functions reasonably believes that it is necessary not to comply with cross-border transfer requirements.

12. https://www.legislation.vic.gov.au/in-force/acts/health-records-act-2001/046
13. https://ovic.vic.gov.au/wp-content/uploads/2019/11/IPP-9-2019.B.pdf

Bangladesh

In Bangladesh, data localisation requirements are sector specific such as information technology and banking. The Data Protection Act of Bangladesh is in draft stage and, once enacted, may include a provision on storing sensitive, user generated and classified data of Bangladesh and its citizens only within the country.

Legislation:

Cloud Computing Policy (Draft)[14]

Key points:

Some key highlights of the legislation are:

Applicable sectors
All sectors handling personal information

Regulatory body
Ministry of Information & Communication Technology

Year of enforcement
Bill is yet to pass

Retention period
Not defined

Penalties
Not defined

14. https://globaldataalliance.org/wp-content/uploads/2021/07/05122021gdabdcloudpol.pdf

Summary

Information that is personal, sensitive, or part of the country's critical infrastructure cannot be taken outside Bangladesh for even backup and retrieval purposes, and the cloud service provider's primary storage location shall be Bangladesh.

Applicability

The Cloud Computing Policy will be applicable to all sectors that deal with personal information.

Type of data

Personal data about an individual, which may include, contact details such as email ID, mobile number, address, financial details such as bank account number, Government ID cards, biometric data, health information, racial or ethnic origin etc., and critical infrastructure related data.

Requirements

The primary location of a cloud service provider's data storage must be in Bangladesh.

Information may be allowed to be taken outside Bangladesh for backup and retrieval purposes where such information does not have any personal or sensitive information, or the information is not deemed harmful to the security and critical information infrastructure of Bangladesh. Further, data sent outside Bangladesh shall only be stored in countries where the Government of Bangladesh has multilateral or bilateral relations for unconditional and instantaneous laws to prevail.

Penalties

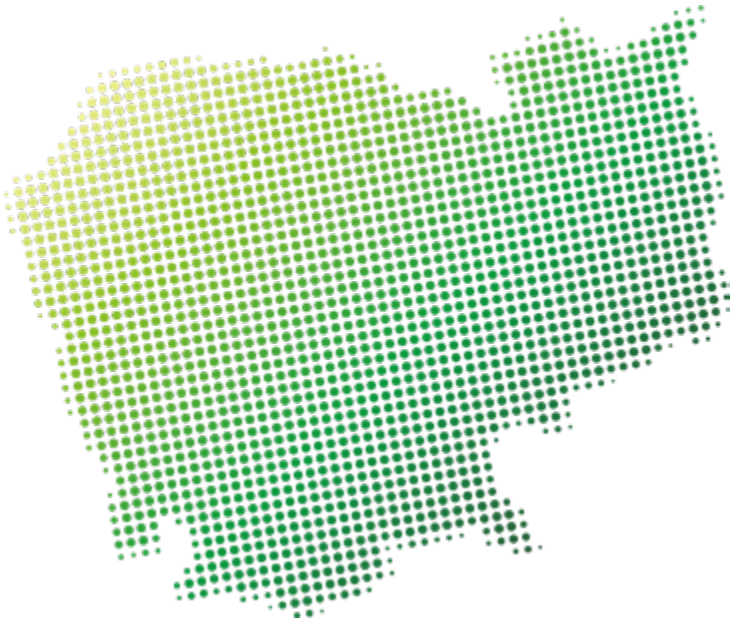
Penalties are not defined in the proposed draft

Exemptions

Not applicable

Cambodia

Data localisation is an integral part of Cambodia's privacy framework under the Law on Electronic Commerce, which mandates that personal data transfers can only take place based on certain conditions as mentioned in the law.



Legislation:

Law on Electronic Commerce[15]

Key points:

Some key highlights of the legislation are:

Applicable sectors

This law applies to all activities, documents and civil and commercial transactions that are made via electronic systems

Regulatory body

Ministry of Commerce

Year of enforcement

2020

Retention period

Not defined

Penalties

The punishment for those who store information in an electronic form for a personal purpose which is contrary to the provisions of this Act will be imprisoned between 1 to 2 years and face a fine ranging from 2,000,000 Riel to 4,000,000 Riel.

15. https://commerce-cambodia.com/2021/06/13/law-on-electronic-commerce-of-kingdom-of-cambodia/

Summary

Only if authorised by the owner or by law, personal data in electronic form can be used, disclosed, and accessed. Further, data in an electronic system cannot be accessed without the permission of the person under whose retention the system is.

Applicability

This law applies to all activities, documents and civil and commercial transactions that are made via electronic systems except for the activities, documents and transactions related to the following:

1. Formation or enforcement of a Power of Attorney
2. Formation or execution of a testament, codicil or other matters relating to succession
3. Any contract for the sale, transfer, or disposition of rights to immovable property or any interests in such property
4. Transfer of immovable property or any interests relating to the immovable property
5. Any other exceptions as provided for by a Sub-Decree.

Type of data

This policy applies to all data including personal data already in existence whether or not by electronic means.

Requirements

Personal information held in electronic form shall be protected by such security safeguards as reasonable in every circumstance to avoid loss, access, use, modification, leak, disclosure of it except with the permission of the owner or of any other person authorised by law.

Further, no person shall interfere in the electronic system and access, retrieve, copy, extract, leak, delete or modify data, which is under the retention of any other person in bad faith or without permission.

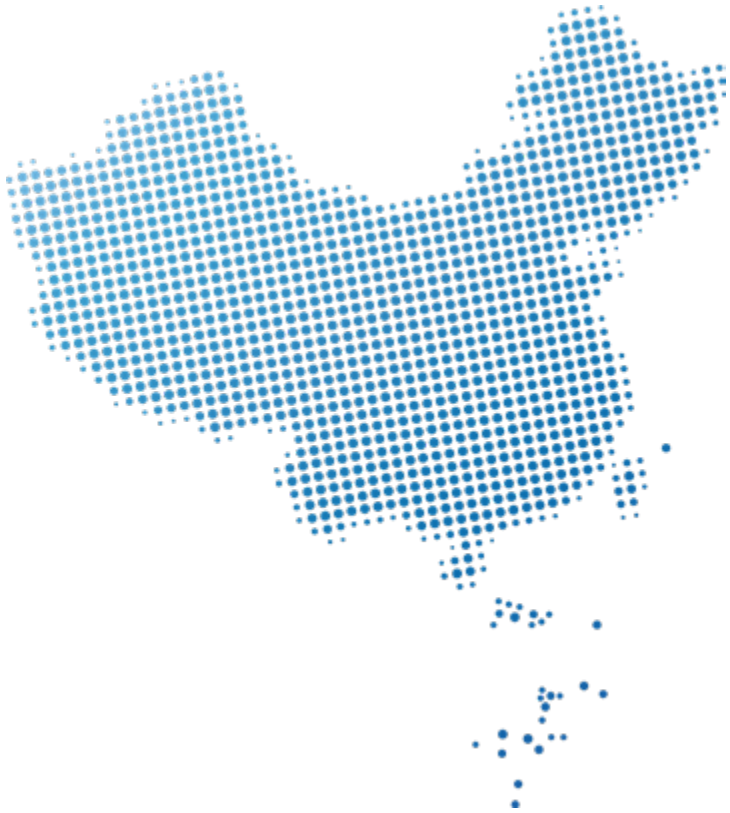
Penalties

The punishment for those who store information in an electronic form for a personal purpose which is contrary to the provisions of this act will be imprisoned between 1 to 2 years and face a fine ranging from 2,000,000 Riel to 4,000,000 Riel.

Exemptions

Not applicable

China



In China, data localisation requirements are found in various sectors such as finance, banking, data protection, technology, publishing and in the automotive industries.

Requirements endorsed by the applicable laws must be complied with for international data transfers and data storage requirements. These laws cover a wide range of information which includes personal data, financial data, important data that is critical to the infrastructure of China, and details published by online publishers.

Applicable regulations

Cybersecurity Law of the People's Republic of China (Law):[16]

Applicability:
This law is applicable to network operators and businesses in 'critical sectors.' Network operators are defined as network owners, managers, and providers; a network is defined as any system comprising computers and related equipment that gathers, stores, transmits, exchanges, or processes information.

Requirements:
This law is regulated by the **Cyberspace Administration of China** and came into force in 2017. It mandates that personal information and important data collected by operators of critical information infrastructure shall be stored within the territory of the People's Republic of China (PRC). If it is necessary for such information to go overseas, a security assessment shall be conducted in accordance with the methods of the Cyberspace Administration of China in conjunction with relevant departments of the State Council.

Type of data:
This is applicable to personal data and important data pertaining to the public communications and information services, energy, finance, transportation, water conservation, public services, and e-governance sectors of China.

Penalties:
If operators of critical information infrastructure fail to perform their cybersecurity protection obligations under this law, the relevant competent departments shall order corrections and give warnings. Those who refuse to make corrections or cause harm to network security and other consequences shall be fined not less than 100,000 yuan but not more than 1,000,000 yuan, and the person in charge who is directly responsible shall be fined not less than 10,000 yuan but not more than 100,000 yuan.

Exemptions:
Not applicable

16. http://www.cac.gov.cn/2016-11/07/c_1119867116_2.htm

Personal Information Protection Law (Law):[17]

Applicability:
This law applies to the activities of processing personal data within the PRC as well as to data processing outside of the PRC, provided that it concerns the processing of personal data of any Chinese resident for the purposes of:

1. Providing goods or services to Chinese residents
2. Analysing or evaluating Chinese residents' behaviour
3. Other circumstances under the laws and regulations.

Requirements:
This law is regulated by the **Cyberspace Administration of China** and came into force in 2021. It mandates that when Critical Information Infrastructure Operators and Personally Identifiable Information processors process personal data that exceeds the amount set by the Cyberspace Administration of China, the personal information collected and processed shall be stored domestically in the People's Republic of China.

Type of data:
This is applicable to personal data.

Penalties:
A violation of this law may result in fines of up to 5% of annual revenue of the previous year or 50 million yuan.

Exemptions:
Not applicable

Data Security Law of People's Republic of China (Law):[18]

Applicability:
This law applies to data handling activities and their security regulation within the mainland territory of the People's Republic of China.

Requirements: The law is regulated by the **Cyberspace Administration of China** and came into force in 2021. The provisions of the Cybersecurity Law of the People's Republic of China apply to the outbound security management of important data collected or produced by Critical Information Infrastructure operators operating within the mainland territory of China. The outbound security management measures for other data handlers collecting or producing important data within the mainland territory of China are to be jointly formulated by the national cybersecurity and informatisation department and relevant departments of the State Council.

Type of data:
This is applicable to important data pertaining to the public communications and information services, energy, finance, transportation, water conservation, public services, and e-governance sectors of China.

Penalties:
A fine of between 100,000 and 1,000,000 yuan may be imposed; a suspension of relevant operations, suspension of operations for rectification, or revocation of relevant business permits or licenses may be ordered; and directly responsible management personnel and other directly responsible personnel can be fined between 100,000 and 1,000,000 yuan.

Exemptions:
Not applicable

17. https://www.lw.com/admin/upload/SiteAttachments/Alert%202894.v5.pdf
18. https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/#_ftn2

Provisions on the Administration of Online Publishing (Law):[19]

Applicability:
This law applies to online publishing services provided within the territory of the People's Republic of China. For the purposes of this law, "online publishing services" means the provision of online publications to the public through information networks.

Requirements:
This law is regulated by the **State Administration for Radio, Film and Television (SARFT)** and came into force in 2016. It mandates that a publisher of a book, audio visual, electronic, newspaper or periodical shall ensure that they have necessary technical equipment for the provision of publishing services and their relevant servers and storage devices are stored within the territory of China.

The law also states that when an application is submitted for online publishing services, it should include the commitment to store the relevant storage devices within the territory of China.

Type of data:
This law applies to data in books, audio visuals, electronics, newspapers, or periodicals of publishers that provide online publishing services.

Penalties:
Not applicable

Exemptions:
Not applicable

Measures on the Automotive Data Security Management (Law):[20]

Applicability:
These measures apply to Operators in automobile design, manufacturing, and service enterprises or institutions, including automobile manufacturers, component and software providers, dealers, maintenance organisations, online car-hailing companies, and insurance companies.

Requirements:
This law is regulated by the **Cyberspace Administration of China**. The law mandates that operators in the Automobile industry and insurance companies shall store personal data and important data within the territory of China. If it is necessary to transfer personal and important data overseas, the operators must undergo the outbound data security assessment organised by the State Cyberspace Administration.

Type of data: This law applies to the personal data of car owners, drivers, and passengers, pedestrians, as well as various information that can infer personal identity and describe personal behaviour. This law also applies to the following types of important data:

1. Data in important sensitive areas such as military management zones, national defence science, technology units and government agencies
2. Surveying and mapping data that is of a higher accuracy than the publicly released maps of the state
3. Operating data of the car charging network
4. Data such as the types of vehicles and the flow of vehicles on the road
5. External audio and video data including faces, voices, and license plates.

Other data that may affect national security and the public interest as specified by the Cyberspace Administration of China and relevant departments of the State Council.

Penalties:
Not applicable

Exemptions:
Not applicable

19. http://lawinfochina.com/display.aspx?id=21941&lib=law
20. http://www.gov.cn/xinwen/2021-05/12/content_5606075.htm

Circular of the People's Bank of China on the Protection of Personal Financial Information by Banking Financial Institutions (Law):[21]

Applicability:
This law is applicable to the personal financial information that is collected, used, stored, and transferred by banking financial institutions.

Requirements:
This law is regulated by the **People's Bank of China** and came into force in 2011. It mandates that personal financial information that is collected within the territory of China shall be stored within the territory of China. However, if provided by any other laws and regulations or the People's Bank of China, banking financial institutions will be allowed to send personal financial information outside the territory of China.

Further, if banking financial institutions enter into agreements with outsourcing service providers, they must ensure that these agreements include all necessary data protection obligations that must be followed by the service provider. These agreements must also include requirements of the service providers to destroy the personal financial information upon the termination of the agreement.

Type of data:
This law applies to Personal Financial Information (Personal Data, Financial Data and Property Data)

Penalties:
Not applicable

Exemptions:
Not applicable

Regulations on the Administration of the Credit Investigation Industry (Law):[22]

Applicability:
This law applies to credit reporting businesses and related activities engaged within the territory of China.

Requirements:
This law is regulated by the **State Council** and came into force in 2013. It states that all information collected by credit reporting establishments in China must be processed and preserved within the territory of China itself. Further, if credit reporting establishments need to send information overseas, they must comply with the laws, administrative regulations, and relevant provisions of the State Council's credit reporting industry supervision and management department.

Type of data:
This law applies to credit information of individuals

Penalties:
Not applicable

Exemptions:
Not applicable

21. http://www.gov.cn/gongbao/content/2011/content_1918924.htm
22. http://www.gov.cn/zhengce/2013-01/29/content_2602614.htm

Interim Measures for the Management of Business Activities of Online Lending Information Intermediaries (Law):[23]

Applicability:
This law applies to online lending information intermediary business activities within the territory of China, except as otherwise provided by laws and regulations.

Requirements:
This law came into force in 2016 and is regulated by the following bodies:

1. The Banking Regulatory Authority of the State Council and its dispatched offices are responsible for formulating supervision and management systems for the business activities of online lending intermediaries.
2. The Provincial-level people's governments are responsible for the institutional supervision of online lending information intermediaries within their respective jurisdictions.
3. The Ministry of Industry and Information Technology is responsible for supervising the telecommunications business involved in the business activities of online lending information intermediaries.
4. The Ministry of Public Security takes the lead in supervising the security of internet services provided by online lending information intermediaries, investigates and punishes illegal activities that violate network security supervision laws, as well as financial and related crimes involved in online lending.
5. The Cyberspace Administration of China is responsible for supervising financial information services, internet information content and other businesses.

This law states that the storage and processing of all lender and borrower information that is collected in China must be carried out within the territory of China itself. Domestic lender and borrower information can only be transferred overseas if it is mandated under other laws or regulations of the country. Loan information of the borrower, the content of information exchanged, and other data must be retained for 5 years from the expiration of the loan contract. Further, the loan contracts must be retained for 5 years after their expiration.

Type of data:
This law applies to lender and borrower data

Penalties:
If online lending information intermediaries violate laws, regulations and relevant supervision provisions on online lending that have penalties, they shall be punished in accordance with those provisions. If relevant laws and regulations do not provide penalties, the local financial supervision department of the place where the industry and commerce registration are located shall determine the punishment. Supervisory measures that can be applied include supervisory conversations, verbal warnings, warning letters, correction orders, circulating a notice of criticism, holding records of violations of laws and regulations and non-fulfilment of public commitments in integrity files and publishing them, fines of not more than 30,000 yuan, and others as specified in the law. Where a crime is deemed to have been committed, criminal responsibility shall be investigated and handled according to the relevant law.

Exemptions:
Not applicable

23. http://www.gov.cn/gongbao/content/2017/content_5181095.htm

The Ministry of Transport and other 10 Departments on the Encouragement and Regulation on the Development of Internet Rental Bicycles Guidance (Law):[24]

Applicability:
Not available

Requirements:
This law is regulated by the **Ministry of Transport** and came into force in 2017. It mandates that all internet rental bicycle operating enterprises that collect information such as personal information and other relevant data in the course of their domestic operations must be stored in the territory of the Chinese Mainland.

Type of data:
This law applies to personal and other relevant data.

Penalties:
Not applicable

Exemptions:
Not applicable

Measures for the Administration of Population Health Information (Trial Implementation):[25]

Applicability:
These measures apply to efforts to collect, manage, use, secure, and protect population health information involved in all types of medical and health family planning service establishments at all levels.

Requirements:
These measures came into force in 2014 and are regulated by the following bodies:

1. Administrative Departments for the Health and Family Planning of people's governments at the county level and above.
2. The National Health and Family Planning Commission responsible for formulating national population health information development plans and management norms, and the overall planning and guiding the management of population health information throughout the country.
3. The health and family planning administrative departments of local people's governments at or above the county level are responsible for promoting, guiding, and supervising the management of population health information in their respective administrative regions.

These measures mandate that population health information must not be stored in servers overseas, and servers that are not hosted or leased abroad.

Type of data:
These measures apply to health data

Penalties:
Not applicable

Exemptions:
Not applicable

24. http://www.gov.cn/xinwen/2017-08/03/content_5215640.htm
25. http://www.cac.gov.cn/2014-08/20/c_1112064075.htm

General Provisions of the Interim Measures for the Administration of Online Taxi Booking Business Operations and Services (Law):[26]

Applicability:
This law applies to those engaged in the operation of online reservation taxis (hereinafter referred to as online taxis).

Requirements:
This law is regulated by the **Ministry of Transport** and came into force in 2016. It mandates that ride-hailing platform companies shall comply with the relevant State network and information security provisions and requires that the personal information collected and the business data generated shall be stored and used in mainland China for a period of not less than 2 years and must not be used or released unless otherwise provided for by laws and regulations.

Type of data:
This law applies to personal and business data

Penalties:
If an online car-hailing platform company violates the above-mentioned requirements, penalties shall be imposed. Those who cause losses to an information subject shall bear civil liability according to the law and those suspected of committing a crime shall be investigated for criminal responsibility in accordance with the law.

If an online car-hailing platform company and an online car-hailing driver illegally use or leak the personal information of car-hailing person and passengers, the public security, network information and other departments shall impose a fine of not less than 2,000 yuan but not more than 10,000 yuan in accordance with their respective duties; if any loss is caused to the information subject, civil liability will be borne according to the law; and if a crime is suspected, criminal responsibility shall be investigated in accordance with the law.

Exemptions:
Not applicable

26. http://www.gov.cn/xinwen/2016-07/28/content_5095584.htm

Map Management Regulations (Law):[27]

Applicability:
This law applies to organisations or individuals in the territory of China that engage in the compilation, review, publication, and supervision and inspection activities of maps disclosed to the public, including through internet map services.

Requirements:
This law is regulated by the **State Council** and came into force in 2016. It mandates that units and individuals within China must not export or send maps out of the country that do not conform to the relevant national standards or regulations of China. Further, the law states that all internet map service units that store map data shall only store them on servers that are located within the territory of China.

Type of data:
This law applies to map related information

Penalties:
If a map violates the provisions of this act by not meeting the relevant national standards and regulations after review and is released to the public without being revised in accordance with the review requirements, the relevant party shall be ordered to make corrections, be given a warning, and have the illegal maps or products with map graphics attached be confiscated. A person may be charged with a fine of less than 100,000 yuan. If there is any associated illegal income, the illegal income will be confiscated. If the circumstances are serious, orders can be made to suspend the business for rectification, lower the qualification level or revoke the surveying and mapping qualification certificate, and the public may be notified of the same. If a crime is deemed to have been committed, criminal responsibility shall be investigated in accordance with the law.

Exemptions:
Not applicable

Terminology	Definitions
Critical Information Infrastructure	Any information infrastructure that can endanger national security, national strategy, and civil welfare in the event of a data breach, compromised network, or system malfunction.
Important Data	Any data that exists in electronic form and may endanger national security and public interests once it is tampered with, destroyed, leaked, or illegally obtained or used.

27. http://www.gov.cn/zhengce/content/2015-12/14/content_10403.htm

Hong Kong SAR

The data localisation requirements are governed by the Personal Data (Privacy) Ordinance (PDPO) under which personal data transfers outside Hong Kong are restricted unless safeguards mentioned under Section 33 of the Ordinance are followed. However, Section 33 of the PDPO is not yet in force.

Legislation:

Personal Data (Privacy) Ordinance (Cap. 486)[28]

Key points:

Some key highlights of the legislation are:

Applicable sectors

All sectors handling personal information

Regulatory body

Office of the Privacy Commissioner for Personal Data

Year of enforcement

1996

Retention period

Personal data should not be kept for longer than is necessary to fulfil the purpose for which the personal data is being processed

Penalties

Contravention of certain provisions of the PDPO are potentially criminal offences; some of the offences that come with heavier penalties are those related to direct marketing and 'doxing'. Offenders may be liable to a maximum fine of HK$1,000,000 and a maximum imprisonment sentence of 5 years.

28. https://www.elegislation.gov.hk/hk/cap486!en-zh-Hant-HK.pdf?FROMCAPINDEX=Y

Summary

The PDPO prohibits personal data transfers outside of Hong Kong unless several conditions are met. However, this provision is not yet in force. Until then, there are currently no formal restrictions imposed on personal data transfers outside of Hong Kong.

Applicability

The PDPO is the main legislation in Hong Kong that aims to protect the privacy of individuals through a set of Data Protection Principles (DPP). The PDPO applies when the collection or processing of personal data is controlled by a data user in Hong Kong, irrespective of the country where the collection or processing is occurring. There is no explicit provision in the PDPO that deals with extra territorial application of the Ordinance.

Type of data

This Ordinance applies to the personal data of individuals

Requirements

Though the provision for data transfers under this Ordinance is not in force as of now, the requirement states that a data user shall not transfer personal data to a place outside Hong Kong unless:

1. The place where the transfer is taking place is specified in a notice
2. There are reasonable grounds for believing that there is a law in force that is substantially similar to, or serves the same purposes as, the PDPO
3. The data subject has consented in writing to the transfer; and
4. The user has reasonable grounds for believing that, in all the circumstances of the case:
   i. The transfer is for the avoidance or mitigation of adverse action against the data subject
   ii. It is not practicable to obtain the consent in writing of the data subject to that transfer; and
   iii. If it was practicable to obtain such consent, the data subject would give it.

The requirements of the Ordinance also state that the Commissioner may, by notice in the Gazette, specify the following on reasonable grounds:

1. The name of a place outside Hong Kong that has a law that is substantially similar to or serves the same purposes as the PDPO.
2. The name of a place outside Hong Kong that no longer has a law that is substantially similar to or serves the same purposes as the PDPO.

Penalties

While contravention of a DPP is not an offence, there are scenarios where the violation of specific provisions of PDPO is an offence.

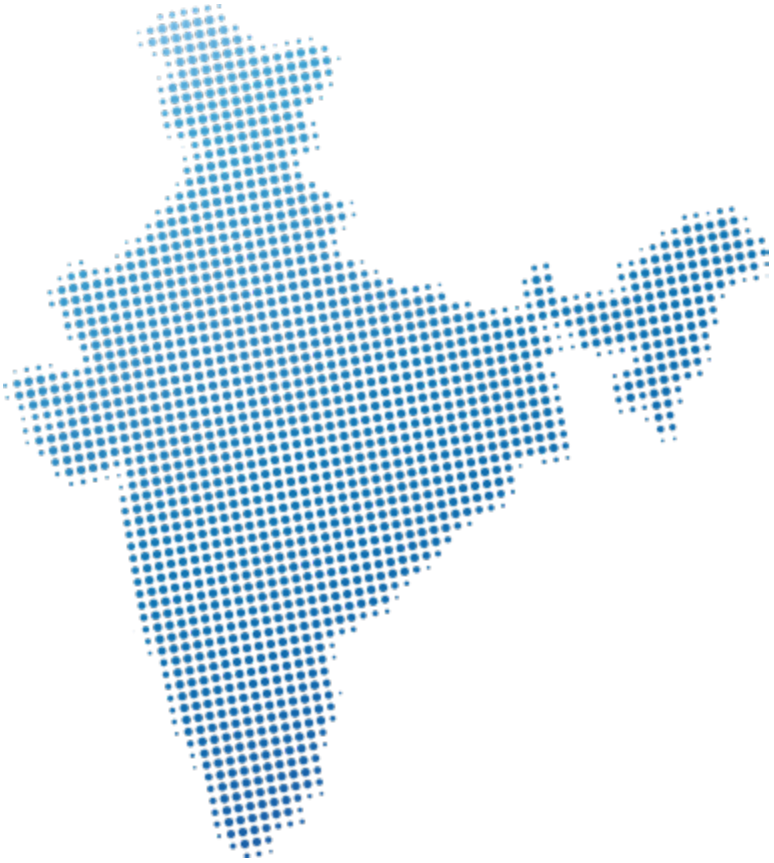
Commissioners conduct investigations if they receive a complaint, or they have reasonable grounds to believe there may be a contravention of the PDPO. Data users found to be contravening or have contravened the PDPO may be given an enforcement notice.

Contravention of an enforcement notice issued by the Commissioner is also an offence which may result in a maximum fine of HK$50,000 and imprisonment for 2 years, with a daily penalty of HK$1,000. Subsequent convictions can result in a maximum fine of HK$100,000 and imprisonment for 2 years, with a daily penalty of HK$2,000.

Exemptions

Not applicable

India



India has the Information Technology ACT (SPDI Rules), which provide guidelines on the transfer of sensitive personal data. There are sectoral laws for banking and insurance, which provide specific requirements on data localisation.

Requirements endorsed by the applicable laws must be complied with for international data transfers and for the storage of data. These laws cover a wide range of information which includes the financial information of companies, credit/ debit card information, personal information, health Information and geospatial data.

Applicable regulations

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) [read with Section 72 and 72A of the Information Technology Act, 2000][29]:

Applicability:
The provisions of the SPDI Rules apply to all bodies corporate and individuals acting on behalf of bodies corporate that collect, receive, possess, store, deal, or handle the personal information of natural persons in India. If a body corporate is located outside of India, the SPDI Rules will only be applicable if the body corporate has a computer, computer system or computer network located in India.

Requirements:
Information defined as sensitive personal data or information (SPDI) can only be transferred to a body corporate or person in India or to one outside India that ensures the same level of protection as stated under the SPDI Rules. The transfer may be allowed if it is necessary for the performance of a lawful contract, or an individual has consented to the transfer.

Type of data:
This Act applies to sensitive personal data or information (SPDI), such as passwords, financial information, medical records and history, biometric information, and call data records.

Penalties:
1. Under Section 72 of the IT Act 2000, the breach of confidentiality and privacy will result in a penalty of either a term of imprisonment which may extend to two years, or with a fine which may extend to one lakh rupees, or both.
2. Under Section 72A of the IT Act 2000, the disclosure of information in breach of a lawful contract will result in a penalty of either a term of imprisonment which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

Exemptions:
Not applicable

29. https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf read with https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

Companies Act, 2013[30]

Applicability:
This Act applies to all public and private sector companies that are incorporated under the Companies Act or any prior law, and to any other companies governed by special laws or as designated by the Central Government.

Requirements:
Section 94 mentions that the registers required to be kept and maintained by a company and copies of the annual return filed shall be kept at the registered office of the company, provided that such registers or copies of the annual return may also be kept at any other place in India in which more than one-tenth of the total number of members entered in the register of members reside.

Type of data:
This applies to the personal data of members who are equity and preference shareholders, debenture holders and any other security holders. This Act also applies to financial data such as the annual returns of a company.

Penalties:
If the making of any extract or copy required under section 94 is refused, the company and every officer of the company who is in default shall be liable, for each such default, to a penalty of one thousand rupees for every day subject to a maximum of one lakh rupees during which the refusal or default continues.

Exemptions:
Not applicable

Rule 3 of the Companies (Accounts) Rules 2014 (read with Section 128 of the Companies Act, 2013)[31]:

Applicability:
Applies to all companies that are incorporated under the Companies Act or any prior law, insurance companies, banking companies, electric companies, and any other companies governed by special laws or as designated by the Central Government.

Requirements:
Backups of the books of account, financial statements and any other books and papers of a company including those that are maintained outside India shall be kept in servers physically located in India on a periodic basis.

Type of data:
These rules apply to the financial information of companies

Penalties:
Punishable with imprisonment for a term which may extend to one year or with a fine which shall not be less than fifty thousand rupees, but which may extend to five lakh rupees, or with both.

Exemptions:
Not applicable

30. https://www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf
31. https://www.mca.gov.in/Ministry/pdf/NCARules_Chapter9.pdf

Reserve Bank of India's Directive 2017-18/153 (read with Section 10(2) and Section 18 of the Payments and Settlement Systems Act, 2007)[32]

Applicability:

This Directive applies to all banks operating in India; and to Payment System Providers (PSPs) authorised by the Reserve Bank of India (RBI) to operate systems in India; and to all other entities in the payment ecosystem, engaged by the PSPs, who provide payment services.

Requirements:

All system providers shall ensure that the entire data relating to the payment systems operated by them are stored in systems located only in India. This data should include the full end-to-end transaction details/ information collected/carried/processed as part of the message/payment instruction. For the foreign leg of a transaction, if any, the data can also be stored in the foreign country, if required.

The Directive lays down that:

1. Payment transactions may be processed outside India. However, the data pertaining to such transactions can only be stored in India.
2. Such data should be deleted from the systems abroad and brought back into India for local storage within 1 business day or 24 hours from payment processing, whichever is earlier.
3. Data pertaining to activities undertaken subsequent to payment processing (such as settlement processing) should also be stored only in India.
4. For cross-border transactions that have both domestic as well as foreign components, a copy of the data pertaining to the domestic component may also be stored overseas, if required.
5. RBI approval is required to share payments data with an overseas regulator.

Type of data:

This applies to payment data such as:

1. Customer data – name, mobile number, email address, Aadhar number, Permanent account number (PAN)
2. Bank account details – customer and beneficiary account details
3. Payment credentials – one-time password (OTP), PIN, passwords, and so on
4. Transaction data – transaction reference, timestamp, underlying amount, originating and designation system information, etc.

Penalties:

Punishable with a fine which may extend to ten lakh rupees, and where a contravention or default is a continuing one, with a further fine which may extend to twenty-five thousand rupees for every day after the first during which the contravention or default continues.

Exemptions:

Not applicable

32. https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244 read with https://m.rbi.org.in/scripts/FAQView.aspx?Id=130

Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015[33]:

Applicability:
Applies to all types of Insurers as mentioned under The Insurance Act, 1938.

Requirements:
The Regulations state that records, including those in electronic mode that pertain to all policies issued and all claims made in India shall be stored in data centres that are located and maintained only in India.

Type of data:
This applies to all records, including those in electronic format, pertaining to insurance policies issued and claims made in India

Penalties:
Not applicable

Exemptions:
Not applicable

Guidelines for Acquiring and Producing Geospatial Data and Geospatial Data Services including Maps[34]:

Applicability:
These guidelines are applicable to geospatial data, maps, products, solutions, and services offered by government agencies, autonomous bodies, academic and research institutions, private organisations, non-Governmental organisations, and individuals.

Requirements:
For foreign entities and foreign owned or controlled Indian companies, there is a certain threshold value for the geospatial data that can be accessed and used by them to cater to their customers in India. The access will only be made available through application programming interfaces (APIs) so that such data does not pass through the foreign companies or their servers. Maps/geospatial data of spatial accuracy/value finer than the threshold value can only be used for the purpose of serving their customers in India. Access to such maps/geospatial data shall only be made available through APIs that do not allow maps/geospatial data to pass through a licensee company or its servers. Re-use or resale of such map data by licensees is prohibited.

Type of data:
These guidelines will be applicable to geospatial data

Penalties:
Not applicable

Exemptions:
Not applicable

33. https://www.irdai.gov.in/admincms/cms/frmGeneral_Layout.aspx?page=PageNo2604&flag=1
34. https://dst.gov.in/sites/default/files/Final%20Approved%20Guidelines%20on%20Geospatial%20Data.pdf

Indonesia

In Indonesia, data localisation requirements are governed by independent laws published by respective regulatory bodies. Organisations must comply with requirements endorsed by such sectoral laws before conducting international data transfers.

Applicable regulations

Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems[35]:

Applicability:
This regulation applies to Electronic System Operators (ESOs). An ESO is any person, state apparatus, business entity and community who/which provides, manages, and/or operates an electronic system which processes personal data either individually or collectively.

Requirements:
This regulation, administered by the **Ministry of Communication and Information Technology (MOCI)**, came into force in 2016 and states that personal data may be transferred outside of the jurisdiction of the Republic of Indonesia only after the following requirements have been fulfilled:

1. Coordination of the data transfer process with MOCI, which includes:
   i. Submitting a report on the implementation plan for the personal data transfer, including details such as the receiving country, recipient's identity, date of implementation, and purpose of transfer
   ii. Requesting advocacy* (if necessary); and
   iii. Submitting a report on the transfer implementation*.
2. Implementation of all applicable provisions governing cross-border data transfers under Indonesian laws and regulations.

**Note: There is lack of guidance and examples from MOCI on advocacy and reports on transfers.*

Type of data:
This applies to any information which either directly or indirectly identifies an individual

Penalties:
Administrative sanctions in the form of:

1. A verbal or written warning
2. Temporary suspension of activities; and/or
3. Announcements on online sites (website).

Exemptions:
Not applicable

35. https://openresearch-repository.anu.edu.au/handle/1885/277084

The new Government Regulation of the Republic of Indonesia No. 71 of 2019 ("GR 71/2019")[36]:

Applicability:

This regulation applies to the following entities which store data on electronic systems:

1. Any public ESO, which is a state institution, or an agency designated by a state institution, that operates an electronic system[37]
2. Any private ESO, which is a private individual, business entity or community that operates an electronic system.

Requirements:

This regulation is administered by the **Ministry of Communications and Informatics (MCIT)** and came into force in 2019. It states that:

1. A public ESO must store its electronic system data in Indonesia, unless the technology needed is unavailable in Indonesia
2. Private ESOs are allowed to manage, process and/or store data in electronic systems outside of Indonesia, subject to the following conditions:
   i. The location of the electronic system and electronic data outside of Indonesia does not diminish the effectiveness of the supervision conducted by a relevant state ministry or institution and law enforcement agencies; below are some effective supervision measures:
      - The Electronic System Operator must have a governance policy, operating procedures, and audit mechanisms that are carried out periodically on the electronic system
      - The Electronic System Operator shall provide an audit track record of all electronic system implementation activities
      - Business actors who carry out electronic transactions may be certified by a Reliability Certification Body (domiciled in Indonesia)

   ii. Access to the electronic system and electronic data must be provided for the purpose of supervision and law enforcement, in accordance with law.

Type of data:

This applies to any data that is stored in electronic format such as images, designs, photos, electronic mail, telegram, numbers, access codes, symbols, and so on.

Penalties:

Only granular administrative sanctions in the form of:

1. Written warnings
2. Administrative fines
3. Temporary suspensions
4. Access termination; and/or
5. Removal from the list of registered electronic system operators.

Exemptions:

Public ESOs that are responsible for regulating and supervising the financial sector are exempted from this regulation.

36. https://peraturan.bpk.go.id/Home/Details/122030/pp-no-71-tahun-2019

37. https://peraturan.bpk.go.id/Home/Download/112816/PP%20Nomor%2071%20Tahun%202019.pdf. (Refer to Chapter 1, Point 1 and 5)

Financial Service Authority of Indonesia – Risk Management Application on Information Technology Utilisation by Commercial Bank (21-06-2016). (NUMBER 18 /POJK.03/2016)[38]:

Applicability:
This regulation is applicable to commercial banks that hold personal information of Indonesian individuals.

Requirements:
Banks are required to locate their electronic system data centres and/or disaster recovery centres domestically. Provided that doing so does not conflict with regulating laws, a bank may have an overseas data centre and/or disaster recovery centre by obtaining an agreement from the Financial Service Authority and fulfilling the requirements of this regulation. Additionally, the transaction processing by a service provider is required to be done domestically.

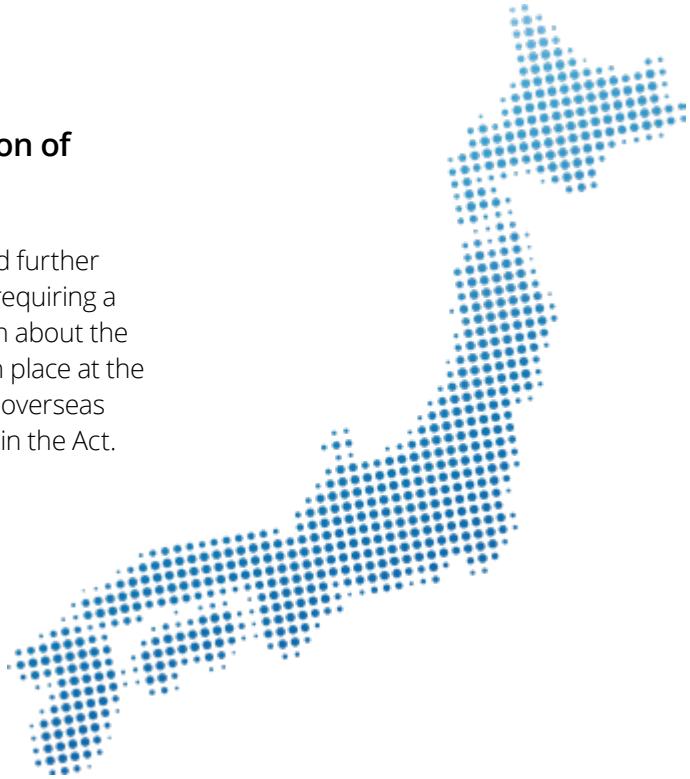
Type of data:
Information held by commercial banks

Penalties:
Not applicable

Exemptions:
Not applicable

38. https://www.ojk.go.id/en/kanal/perbankan/regulasi/peraturan-ojk/Documents/Pages/POJK-concerning-Implementation-of-Risk-Management-for-Commercial-Banks-/POJK%20No.%2018-POJK.03-2016%20Implementation%20of%20Risk%20Management%20for%20Commercial%20Banks.pdf

Japan



As of April 2022, the Amended Act on the Protection of Personal Information came into force.

Japan's Personal Information Protection Committee has released further guidance on the requirements for cross-border data transfers, requiring a data exporter to provide data principals with certain information about the transfer, including the destination country and the safeguards in place at the data importer. So far there are no registration requirements for overseas transfers of data and no general data localisation requirements in the Act.

Legislation:

Act on the Protection of Personal Information (Law)[39]

Key points:

Some key highlights of the legislation are:

Applicable sectors

The law covers both public and private sectors

Regulatory body

Personal Information Protection Commission (PPC)

Year of enforcement

2022 (the most recent amendment)

Retention period

Not specifically defined but when no longer required, data should be deleted

Penalties

100 million Japanese yen or less for Illegally providing/using personal information data or disobeying a PPC order. (There are other penalties for different violations as well.)

Terminology	Definitions
Principal	A "principal" in relation to personal information in this Act means a specific individual identifiable by personal information.

39. https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf

Summary

The amended Act was put into force in April 2022, requiring personal information handling business operators to provide data principals with information about cross border transfer such as the destination country and the safeguards in place at the data importer.

Applicability

The Act applies to personal information handling business operators who process personal information data.

Type of data

Personal information means any information relating to an identified or identifiable natural person, such as a name, an identification number, location data, and an online profile.

Requirements

A personal information handling business operator is allowed to transfer personal information to a third party located in a foreign country if:

1. The foreign country is certified to have a level of data protection comparable to that of Japan (as of April 2022, EU member states and UK), or
2. The personal information handling business operator provides certain information to the data principal(s) regarding the transfer and ensures the third party has safeguards that meet the criteria set by PPC, or
3. The personal information handling business operator receives consent from the data principal after having provided them with the required information about the transfer.

Penalties

100 million Japanese yen or less for Illegally providing and using personal information data or disobeying a PPC order.

(There are other penalties for different violations as well.)

Exemptions

Journalistic organisations, professional writers, academic organisations, religious bodies, and political bodies are not subject to this Act.

Malaysia

In Malaysia, data localisation requirements are found in various sectors such as finance, health care, consumer, and telecommunications. These requirements are governed by independent laws published by respective regulatory bodies.

Organisations must comply with the requirements of such sectoral laws before conducting international data transfers. These laws cover information that includes financial records and personal information.

Applicable regulations

The Personal Data Protection Act 2010 (PDPA):[40]

Applicability:
This law applies to data users (organisations processing data) if they are established in Malaysia (regardless of whether or not the personal data is processed in the context of that establishment). It also applies to data users not established in Malaysia, but which use equipment in Malaysia to process the personal data, except where the purpose is only of transit through Malaysia.

Requirements:
This Act is regulated by the **Personal Data Protection Commissioner (PDP Commissioner)** and came into force in 2010. It introduced requirements over international data transfers which state that transfers of personal data outside of Malaysia may only be done if the receiving country is listed in a published Gazette. (To date, no countries have been published.) Alternatively, personal data can be transferred outside Malaysia if the data subject has given consent to the transfer, for the performance of a contract, for the purpose of any legal proceedings or for the exercising or defending of legal rights, for the mitigation of adverse action against the data subject, if the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in a manner which would be in contravention of the PDPA, to protect the vital interests of the data subject, or if the transfer is in the public interest in circumstances determined by the Prime Minister of Malaysia.

Type of data:
This is applicable to personal data that relates directly or indirectly to an individual who is identified or identifiable from that information, and sensitive personal data that is information as to the physical or mental health condition of an individual, his or her political opinions, or his or her religious beliefs.

Penalties:
Breach of the restrictions on transborder dataflows is an offence that can result in a fine of up to 300,000 Malaysian Ringgit and/or imprisonment for up to 2 years.

Exemptions:
Not applicable

40. https://www.malaysia.gov.my/portal/content/654, https://www.dlapiperdataprotection.com/index.html?t=definitions&c=MY

Income Tax Act 1967:[41]

Applicability:
Persons carrying out business in Malaysia or employed in Malaysia.

Requirements:
This Act is regulated by the **Inland Revenue Board of Malaysia (IRBM)** and came into force in 1967 (fourth reprint in 2006). It mandates that all taxable persons/businesses keep sufficient accounts regarding their liability for income tax in the national language (Malay) or English, and that these documents are retained in Malaysia unless the Director General approves otherwise. This data should be retained for **7 years**.

Type of data:
Tax related documents such as books of account recording receipts and payments, income and expenditure, invoices, vouchers, and receipts, and such other documents as in the opinion of the Director General are necessary to verify the entries in any books of account and any other records as may be specified by the Director General.

Penalties:
Non-compliance with this law can result in a fine of 300 Ringgit – 10,000 Ringgit or imprisonment for a term not exceeding 1 year, or both.

Exemptions:
Not applicable

Goods and Services Tax Act:[42]

Applicability:
Any taxable person, and certain non-taxable persons as per Paragraph 135 of the RMCD Guidelines 2013.

Requirements:
This Act is regulated by the **Inland Revenue Board of Malaysia (IRBM)**, came into force in 2014, and mandates all taxable persons/businesses to keep records which include all records of goods and services provided by a taxable person, all import records, and any other supporting documents such as contracts, or price quotations that affect or may affect said person's liability under the GST Act within Malaysia except as otherwise approved by the Director General. This data should be retained for **7 years**.

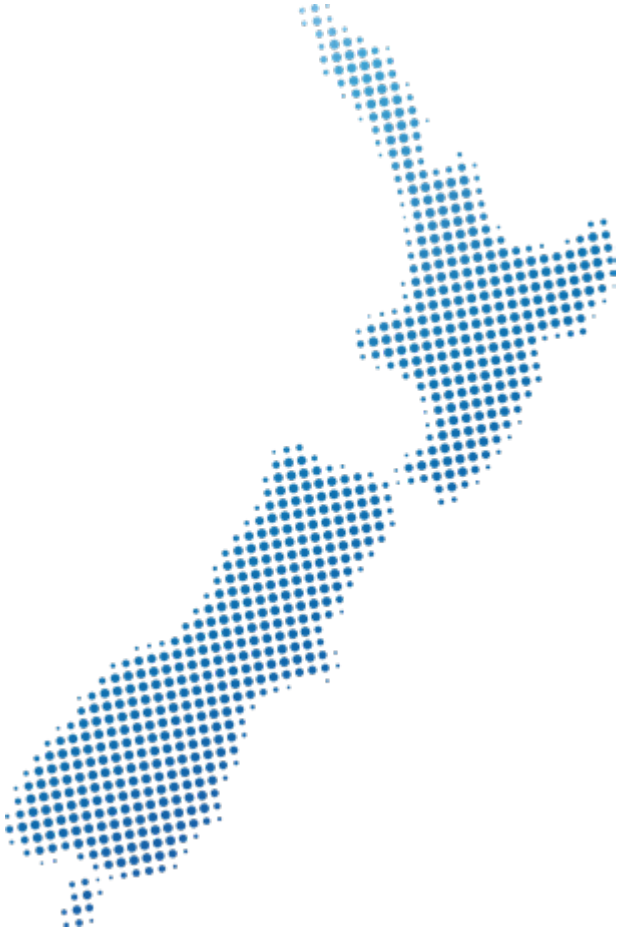
Type of data:
This is applicable to tax related documents such as records of goods and services supplied by or to that taxable person including tax invoices, invoices, receipts, debit notes, credit notes, export declaration forms, records of the importation of goods, and all other records required by the Director General.

Penalties:
Non-compliance with this law can result in a fine of up to 50,000 Ringgit or imprisonment for a term up to 3 years, or both.

Exemptions:
Not applicable

41. https://phl.hasil.gov.my/pdf/pdfam/Act_53_20190101.pdf
42. http://gst.customs.gov.my/en/rg/SiteAssets/gst_actw/GOODS_AND_SERVICES_TAX_ACT_2014v1.pdf

New Zealand



In New Zealand, data localisation requirements are found in various sectors such as finance, health care, consumer, and telecommunications. These requirements are governed by independent laws published by respective regulatory bodies.

Organisations must comply with the requirements endorsed by such sectoral laws before conducting international data transfers. These laws cover a wide range of information, which includes financial records, personal information, health information and Māori data. The latter refers to digital or digitisable information or knowledge that is about or from Māori (Indigenous people) and their language, culture, resources, or environments.

Applicable regulations

Inland Revenue Acts (Tax Administration Act 1994 and Goods and Services Tax Act 1985):[43]

Applicability:
These laws are applicable to an individual who, or an organisation that, carries on a business in New Zealand (including those who do business via the internet).

Requirements:
The **Tax Administration Act 1994** and the **Goods and Services Tax (GST) Act 1985** are regulated by the **Commissioner-Parliamentary Counsel Office New Zealand** and require a taxpayer to keep their business records in New Zealand unless the Commissioner has authorised that those records may be kept offshore. This applies to business records in both paper form and electronic form. These records must be retained for the full retention period required by the Act, currently **7 years** unless extended to **10 years** by the Commissioner for specific situations.

Type of data:
Records which include books of account (whether contained in a manual, mechanical, or electronic format) that record receipts or payments or income or expenditure, and also vouchers, bank statements, invoices, tax invoices, credit notes, debit notes, receipts and any other data associated with GST.

Penalties:
Non-compliance with these regulations may lead to imprisonment of up to 5 years or a fine of up to NZ$50,000, or both.

Exemptions:
Individual businesses may apply for authorisation from the Commissioner before sending their records outside of New Zealand. Authorisation can be given to an individual business to hold their own records offshore or to a third party to hold records for multiple clients offshore. If an individual business wants a third party to hold its records overseas, and that third party already has authorisation, then the individual does not need separate authorisation from the Commissioner.

43. https://www.legislation.govt.nz/act/public/1994/0166/latest/whole.html?search=qs_act%40bill%40regulation%40deemedreg_Tax+Administration+Act+1994+_resel_25_h&p=1#LMS57676
https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html?search=ts_act%40bill%40regulation%40deemedreg_privacy+act_resel_25_a&p=1

The Privacy Act 2020:[44]

Applicability:

This Act is applicable to any agency or organisation that collects personal information in New Zealand, including an overseas agency or organisation that collects data remotely or through another party.

Requirements:

This Act is regulated by **The Office of the Privacy Commissioner (OPC)** and came into force in December 2020 (including different codes of practices), introducing a new requirement on international data transfers. It states that the agency transferring personal data must either believe on reasonable grounds that the recipient is subject to privacy laws that, overall, provide comparable safeguards to those of the New Zealand Privacy Act, or that the recipient is required to protect the information in a way that overall provides comparable safeguards to the Privacy Act (for example pursuant to contract). If a jurisdiction does not offer similar protections, the individual concerned (the data subject) must be fully informed that their information may not be adequately protected, and they must expressly authorise the disclosure.

The Act also mentions that "*prescribed country*" means a country to which data transfer is permitted under the Act, but the OPC has not yet published such a list. The official website of the regulator body does provide a **model clause – template**[45] and model contract clause builder tool which can be used as a transfer mechanism by organisations.

This Act also gives the Privacy Commissioner the power to issue **codes of practice**[46] that become part of the law. These codes modify the operation of the Privacy Act and set rules for specific industries, organisations, or types of personal information. There are currently six codes of practice:

1. Civil Defence National Emergencies (Information Sharing) Code
2. Credit Reporting Privacy Code
3. Health Information Privacy Code
4. Justice Sector Unique Identifier Code
5. Superannuation Schemes Unique Identifier Code
6. Telecommunications Information Privacy Code.

Type of data:

This act is applicable to personal information, which means information about an identifiable individual; it also includes information relating to death as maintained by the Registrar-General.

Penalties:

Non-compliance with these regulations may lead to a fine of up to NZ$10,000, except in the case of class action lawsuits wherein the maximum award by the Human Rights Tribunal is NZ$350,000 for each member of the class action.

Exemptions:

This Act exempts the transfer of personal data when such transfer is in relation to public health, public safety, national security, the maintenance of law and order, and others as described under Privacy Principle 11(1)(e) and (f).[47] Principle 12 – 'Disclosure outside New Zealand' does not apply where the personal information is sent to an agent for storage or processing and the agent does not use or disclose the information for its own purposes (in this case there is no "disclosure" for the purposes of the Act), or if another statute expressly authorises or requires the disclosure of personal information to the foreign person or entity.

44. https://www.legislation.govt.nz/act/public/2020/0031/latest/whole.html?search=ts_act%40bill%40regulation%40deemedreg_privacy+ACt_resel_25_a&p=1#LMS23223
45. https://www.privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/
46. https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/
47. https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23376.html?search=ts_act%40bill%40regulation%40%20deemedreg_privacy+ACt_resel_25_a&p=1

Māori Data Sovereignty Network:[48]

Applicability:
This applies to any organisation processing Māori data.

Requirements:
The purpose of **Te Mana Raraunga (TMR)** is to enable Māori Data Sovereignty and to advance Māori aspirations for collective and individual wellbeing. The idea for Te Mana Raraunga emerged from a meeting of Māori researchers and practitioners at a workshop hosted by the Academy of the Social Sciences in Australia on Data Sovereignty for Indigenous Peoples in July 2015.

Type of data:
This is applicable to Māori data, which refers to digital or digitisable information or knowledge that is about or from Māori people, language, culture, resources, or environments.

Penalties:
Not specified

Exemptions:
Not specified

48. https://www.temanararaunga.maori.nz/

Philippines

Data localisation is an integral part of the privacy framework of the Philippines that is governed by the National Privacy Commission (the "Commission"), under which the international transfer of personal data is restricted unless organisations ensure that the recommended safeguards are in place.

The Data Privacy Act of the Philippines also mentions certain exemptions and transfer mechanisms which can be leveraged by organisations.

Legislation:

Republic Act No. 10173, known as the Data Privacy Act of 2012 (the Data Privacy Act) [49]

Key points:

Some key highlights of the legislation are:

Applicable sectors
All sectors handling personal information

Regulatory body
The National Privacy Commission

Year of enforcement
2012

Retention period
Not defined

Penalties
A fine of five hundred thousand pesos (Php 500,000) to two million pesos (Php 2,000,000) or imprisonment or both.

49. https://www.privacy.gov.ph/data-privacy-act/

Summary

Transfers to other countries are permissible under the Data Privacy Act of the Philippines. However, each Personal Information Controller is responsible for the personal Information under its control or custody, including information that has been transferred to a third party for processing overseas. The Personal Information Controller must use contractual or other reasonable means to provide a comparable level of protection for personal information processed by a third party.

Applicability

The Data Privacy Act and the Implementing Rules and Regulations (IRR) apply to controllers and processors established in the Philippines and the processing of personal data by any natural or juridical person in the government or private sector.

Type of data

Personal information about an individual, which may include contact details such as email address and mobile number.

Sensitive information such as financial details (e.g., bank account numbers), religious beliefs, sexuality, government identity cards, biometric data, health information, and racial or ethnic origin.

Privileged information that is data which falls under the rules of court and other pertinent laws.

Requirements

The Act states that "Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation." A Personal Information Controller or Personal Information Processor is required to register its data processing system(s) and provide certain details about it including whether the personal data it processes would be transferred outside of the Philippines.

Penalties

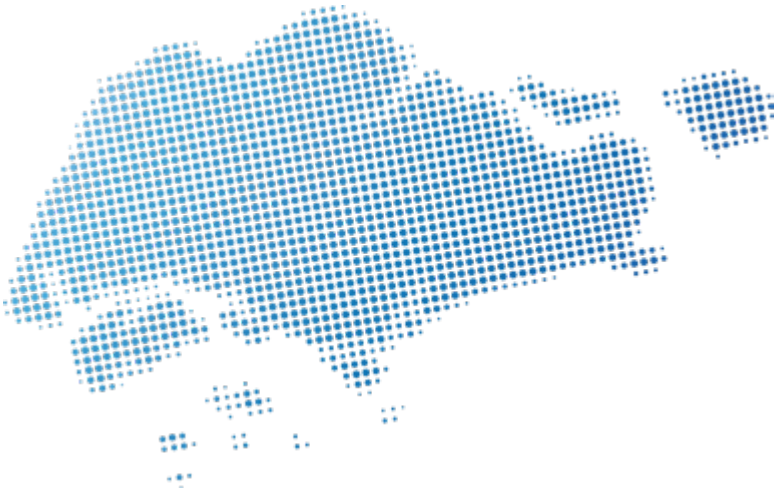
The Commission may impose a fine of between five hundred thousand pesos (Php 500,000) and two million pesos (Php 2,000,000) in a case of non-compliance.

Exemptions

No exemptions are defined

Singapore

The data localisation requirement is an integral part of Singapore's privacy framework. It is governed by the Personal Data Protection Act 2012 (PDPA) under which international personal data transfer is restricted, unless organisations ensure that the required safeguards are in place.



Legislation:

The Personal Data Protection Act 2012 (PDPA)[50], Personal Data Protection (Amendment) Act 2020[51]

Key points:

The Personal Data Protection Act restricts transfer of personal data outside of Singapore, unless appropriate safeguards to protect personal data are in place.

Applicable sectors
All sectors handling personal data

Regulatory body
The Personal Data Protection Commission (PDPC)

Year of enforcement
2012

Retention period
Not defined

Penalties
Currently up to S$1 million. (Higher penalties will come into effect in October 2022).

50. https://sso.agc.gov.sg/Act/PDPA2012?WholeDoc=1
51. Personal Data Protection (Amendment) Act 2020 - Singapore Statutes Online (agc.gov.sg)

Summary

An organisation transferring personal data outside of Singapore must ensure that it has taken appropriate steps to comply with the PDPA obligations in respect of the transferred personal data. Also, it must ensure that the recipient outside of Singapore is bound by legally enforceable obligations to provide a standard of protection over the personal data that is comparable to the PDPA.

Applicability

The PDPA applies to organisations collecting, using and/or disclosing personal data in Singapore, whether or not the organisation itself has a physical presence or is registered as a company in Singapore.

Type of data

Personal data about an individual, which may include contact details such as email address, mobile number, physical address, financial details such as bank account numbers, government identity cards, biometric data, health information, and racial or ethnic origin. Business contact information is not covered by the PDPA.

Requirements

The PDPA states that an organisation must not transfer any personal data to a country or territory outside of Singapore except in accordance with the requirements prescribed under the PDPA to ensure that the recipient organisations provide a standard of protection over the transferred data comparable to that under the PDPA. In essence, an organisation may transfer personal data overseas if it has taken appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations (law, contract, binding corporate rules, or any other legally binding instrument) or specified certifications to provide the transferred personal data a standard of protection comparable to that under the PDPA.

In June 2020, the PDPC amended the Personal Data Protection Regulations 2021 to recognise the Asia Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processor (PRP) certification system as a specified certification and a legally enforceable obligation for transfer of data overseas.

The recipient is considered to have satisfied the requirements for data transfer if they hold the CBPR or APEC PRP certification, or both. Singapore has also developed a model sample contract clause that transferring organisations can include in their contracts with such recipients.[52]

Penalties

The PDPC has a range of powers under the PDPA including directing an organisation/person to pay a financial penalty of up to S$1million. The current maximum financial penalty will be increased from 1 October 2022, when the enhanced penalty provisions come into effect, to the higher of: for an organisation, 10% of the organisation's annual turnover in Singapore (if the organisation's annual turnover in Singapore exceeds S$10 million), or S$1 million; for a person, 5% of the person's annual turnover in Singapore (if the person's annual turnover in Singapore exceeds S$20 million), or S$1 million.

Exemptions

Any person or organisation (or any class of persons or organisations) may be granted exemption from all or any of the provisions of the PDPA with the approval of the Minister, by order published in the Gazette.

52. https://www.pdpc.gov.sg/news-and-events/announcements/2020/06/singapore-now-recognises-apec-cbpr-and-prp-certifications-under-pdpa

South Korea

In South Korea, data localisation requirements are governed by the Personal Information Protection Act and several industry-specific laws. In essence, cross-border data transfers require consent given by the data subject, notification of relevant details, and an information security system which meets the prescribed standards.

Applicable regulations

Act on the Establishment and Management of Spatial Data (Law):[53]

Applicability:
This Act applies to various forms of surveys that are undertaken by individuals and government agencies.

Requirements:
The Act stipulates that no person shall take abroad maps or photos that were produced for the purpose of, or part of the results of, a fundamental or public survey, unless they fall within various stated exceptions within the law. The copies are to remain within the border of the country. Important articles to be considered are Articles 16, 21, 106 and 108.

Type of data:
Spatial data contained in fundamental and/or public survey results

Penalties:
A person who moves the fundamental or public survey results abroad pursuant to the provision to Article 16 and the provision to Article 21 of the Act, as mentioned under Section 108, shall be punished by imprisonment for not more than 2 years or by a fine not exceeding 20 million won.

Exemptions:
Not applicable

53. https://elaw.klri.re.kr/eng_service/lawView.do?hseq=32771&lang=ENG

Personal Information Protection Act (PIPA) (Law):[54]

Applicability:
The Act is applicable to personal information controllers, which means any legal person, organisation, individual or public institution that processes personal information directly or indirectly as part of their activities.

Requirements:
The Act puts forward various rights that individuals can exercise to ensure their data is looked after and shared appropriately with an entity. Entities that handle personal data have the duty to ensure that it does not leave the country unless permission from the data holder is obtained. The same data can only be shared when information is given to the data subject holder about the location of the data transfer. Important Articles to be considered are Articles 17, 39-12, 39-13, 39-15, and 75.

Type of data:
Personal information

Penalties:
A person falling under Article 75 can be charged an administrative fine of up to 20 million won. Under Article 39-15, communications service providers and others can be charged with surcharges not exceeding 3% of the total revenues relating to the concerned violation.

Exemptions:
Not applicable

Act on Promotion of Information and Communications Network Utilisation and Information Protection (Network Act) (Law)[55]

Applicability:
The Act applies to providers of information and communications services, which means any telecommunications business entity defined in the Telecommunications Business Act.

Requirements:
The law mandates that users and information & communications service providers prevent important information from outflowing abroad. Important Articles to consider include Article 51.

Type of data:
Important information means information related to national security and major policies, information about cutting-edge science and technology, or equipment developed within South Korea

Penalties:
Not applicable

Exemptions:
Not applicable

Regulation on Supervision of Electronic Financial Activities (Administrative Rule):[56]

Applicability:
This regulation applies to Electronic Financial Business Operators.

Requirements:
The regulation requires that when financial data is acquired from an individual, the data collection agency and the data processing agency shall have a dedicated server room and a disaster recovery centre that are established within South Korea. The information that is collected from the data subject should always be stored at such locations. Handling of the unique identification information and personal credit information must follow Article 11-11.

Type of data:
Personal information within the financial sector

Penalties:
Not applicable

Exemptions:
Not applicable

54. https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=53044&type=lawname&key=personal+information+protection
55. https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=55570&type=lawname&key=Act+On+Promotion+Of+Information+And+Communications+Network+Utilization+And+Information+Protection
56. https://www.law.go.kr/admRulLsInfoP.do?admRulSeq=2100000174672

Sri Lanka

The personal data protection law of Sri Lanka sets various requirements for public and non-public authorities, as controllers or processors, to restrict the cross-border transfer of personal data. The Act prescribes various measures for a controller or processor to adopt before transferring personal data to another country.

Legislation:

Personal Data Protection Act, No. 9 of 2022 (Law) [57]

Key points:

Some key highlights of the legislation are:

Applicable sectors
All sectors handling personal information

Regulatory body
Data Protection Authority of Sri Lanka

Year of enforcement
2023

Retention period
Not defined

Penalties
Ten million Rupees for each act of non-compliance.

57. https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf

Summary

Information that is personal, sensitive, or part of the country's critical infrastructure cannot be taken outside of Sri Lanka for processing, unless permission has been granted by the relevant authority.

Applicability

The Personal Data Protection Act is applicable to all sectors that deal with personal information.

Type of data

Personal data and specific categories of personal data about an individual, which may include contact details (such as email address, mobile number, and physical address), financial details such as bank account numbers, government identity cards, biometric data, health information, and racial or ethnic origin.

Requirements

Where a public authority processes personal data as a controller or processor, such personal data shall be processed only within the territory of Sri Lanka. The public authority shall not process such personal data in another country unless permitted as per the adequacy decision prescribed by the Minister assigned to the subject of data protection under the Constitution.

A controller or processor other than a public authority may process personal data in a country prescribed pursuant to an adequacy decision. For the purpose of making an adequacy decision, the Minister shall, in consultation with the authority, take into consideration the relevant written law and enforcement mechanisms relating to the protection of personal data in a third country and the application of the provisions of the Act. For transfers to a non-prescribed country the controller or processor must ensure compliance with the required obligations under the Act.

These include the appointment of a Data Privacy Officer (DPO), implementation of appropriate technical and organisational measures, written instructions for the processing of data by a processor, implementing a breach notification process, and a privacy impact assessment.

In the absence of an adequacy decision or the appropriate safeguards, a controller or processor other than a public authority may process personal data outside Sri Lanka if:

1. The data subject has explicitly consented, or
2. The transfer is necessary for the performance of a contract between the data subject and the controller, or
3. The transfer is necessary for the establishment, exercise or defence of legal claims relating to the data subject, or
4. The transfer is necessary for reasons of public interest, or
5. The transfer is necessary to respond to an emergency that threatens the life, health, or safety of the data subject, or
6. Such processing is permitted under any other conditions as may be prescribed under the Act.

Penalties

Ten million Rupees for each act of non-compliance with the law by a data controller and processor. In addition, the Act has a unique penalty in place for repetitive non-compliance with the law. The data controller or processor is liable to pay an additional penalty consisting of twice the amount imposed as a penalty on the second and each subsequent act of non-compliance.

Exemptions

Exceptions to the application of the law are:

1. The protection of national security, defence, public safety, public health, economic and financial systems stability of the Republic of Sri Lanka
2. The impartiality and independence of the judiciary
3. The prevention, investigation, and prosecution of criminal offences
4. The execution of criminal penalties
5. The protection of the rights and fundamental freedoms of persons, particularly the freedom of expression and the right to information.

Taiwan

Taiwan's Personal Data Protection Act mandates that personal data be transferred based on certain conditions as mentioned within the Policy.

Legislation:

Personal Data Protection Act, 2015[58]

Key points:

Some key highlights of the legislation are:

Applicable sectors

All government ministries, departments, educational institutions and statutory boards handling data (called Agencies) and any businesses

Regulatory body

The Policy is under the authority of the National Developmental Council

Year of enforcement

2015

Retention period

Not defined

Penalties

Imprisonment for not more than 5 years and a fine of not more than NT$1 million.

58. https://www.rootlaw.com.tw/en/LawContent.aspx?LawID=A040030000001800-1041230

Summary

The Act governs the collection, transfer, use and storage of personal data by various entities within Taiwan, and stipulates various penalties for non-compliance.

Applicability

The Act applies to all individuals, whether resident in Taiwan or not, whose data is or has been processed by the bodies such as government ministries, educational institutions and statutory boards handling data (called Agencies) and any private businesses.

Type of data

The Act applies to personal data which refers to a natural person's name, date of birth, ID card number, passport number, features, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, data concerning a person's sex life, records of physical examination, criminal records, contact information, financial conditions, data concerning a person's social activities and any other information that may be used to directly or indirectly identify a natural person.

Requirements

While there is no specific mention of data localisation within this legal framework, various standards are prescribed for the international transfer of data. As per the Act, if a cross-border transfer of personal data is carried out by a non-government agency (refers to a natural person, legal person or group) the central government authority in charge of the industry concerned may impose restrictions on transfer of data. They can impose such restrictions when there is a major national interest involved; when an international treaty or agreement so stipulates; when the country receiving the personal data lacks the proper regulations on the protection of personal data and the data subjects' rights and interests may consequently be harmed; or when the cross-border transfer of the personal data is carried out to circumvent the PDPA. The important Articles for this Act are Articles 21 and 41.

Penalties

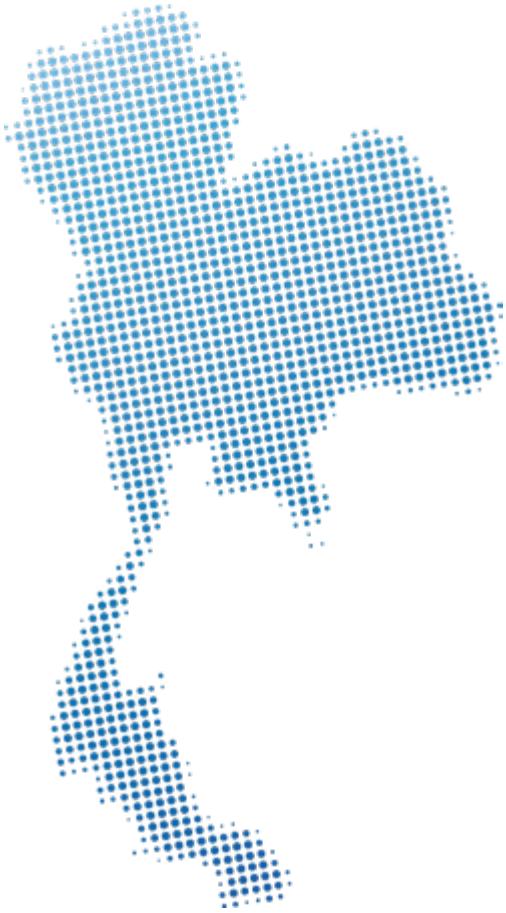
In the case of a violation of Articles 6, 15, 19, 20, or 21 of the PDPA, an individual shall be sentenced to imprisonment for not more than 5 years and a fine of not more than NT$1 million.

Exemptions

The following data processing activities are exempted:

1. Where it is expressly required by law
2. Where the personal data has been disclosed to the public by the data subject or has been made public lawfully
3. Where it is necessary for the gathering of statistics or academic research by a government agency or an academic institution
4. Where it is necessary to assist a government agency in performing its statutory duties or a non-government agency in fulfilling its statutory obligations, provided that proper security and maintenance measures are adopted prior or after such collection, processing, or use of personal data
5. Where the data subject has consented to the collection, processing and use of their personal data.

Thailand



Thailand's Personal Data Protection Act B.E. 2562 (2019) mandates that personal data transfers can only take place based on certain conditions as mentioned in the Act.

Legislation:

The Personal Data Protection Act B.E. 2562 (2019)[59] and 4 subordinate legislations based on announcements of the Personal Data Protection Committee:

1. Criteria and procedure for Record of Processing Activities (ROPA) creation for Data Processor B.E. 2565 (2022)
2. Exemption of Record of Processing Activities (ROPA) for Data Controller classified as Small and Medium-sized Enterprise (SME) B.E. 2565 (2022)
3. Criteria for issuing an administrative fine by expert committee B.E. 2565 (2022)
4. Security Measure for Data Controller B.E. 2565 (2022)

Key points:

Some key highlights of the legislation are:

Applicable sectors

The Act applies to the collection, use, or disclosure of personal data by a data controller or a data processor that is in the Kingdom of Thailand

Regulatory body

The Act is under the authority of the Personal Data Protection Committee

Year of enforcement

2022

Retention period

Not defined

Penalties

Administrative penalty: For minor infringements, a warning and restrictions over the collection, use or disclosure of personal data; fines of up to 5 million Baht for severe infringements.

Criminal penalty: imprisonment ranging from a few months to a year, along with a penalty of up to one million Baht, or both, for criminal charges.

59. https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf

Summary

The Personal Data Protection Act, 2562 B.E. (2019) (Thai PDPA) controls the collection, use, and disclosure (processing) of personal data by establishing a data subject's right to access, delete, and prohibit the processing of their personal data under the responsibility of the organisation. Furthermore, the Thai PDPA requires the organisation to only collect, use or disclose personal data under specified legal bases.

Applicability

The Act applies to the collection, use, or disclosure of personal data by a data controller or a data processor that is in the Kingdom of Thailand.

Type of data

The Act applies to all personal data, that is any information relating to a person which enables the identification of such person, whether directly or indirectly, but not including the information of the deceased persons.

Requirements

The Thai PDPA has several requirements in terms of data disclosure and data transfer to other countries. It states that data collectors shall prevent the unauthorised or unlawful use or disclosure of personal data by a third party. Where a data controller must disclose personal data to another person or legal persons, the controller shall have systems or technical measures in place to resolve any requests from users (data subject right requests). Additionally, the transfer of personal data to another country shall take place only if that country's standard of personal data protection is deemed adequate as per the Thai PDPA (subject to certain exceptions as stated under Exemptions).

Penalties

Any data controller who violates the provisions under the Act in a manner that is likely to cause a person to suffer damage, impair their reputation, or expose such other person to scorn, hatred, or humiliation, shall be punished with imprisonment for a term not exceeding six months, a fine not exceeding five hundred thousand Baht, or both. Any data controller who violates the provisions under sections 27 or 28, which relate to personal data, in order to unlawfully benefit themselves or another person shall be punished with imprisonment for a term not exceeding one year, a fine not exceeding one million Baht, or both.

Any data controller who violates sections 26 or 27 or 28 of the Act shall be punished with an administrative fine not exceeding five million Baht.

Exemptions

The following data processing activities are exempted from the Act:

1. To prevent or suppress a danger to life, body or health of the person, where the data subject is incapable of giving consent for whatever reason.
2. It is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, religious, philosophical, or trade union purpose for their members, including former members of the bodies, or persons having regular contact with such foundations.
3. It is information that is disclosed to the public with the explicit consent of the data subject.
4. It is necessary for the establishment, compliance, exercise or defence of legal claims.
5. It is necessary for compliance with a law for one or more of the following purposes:
   i. Preventive or occupational medicine
   ii. Public interest in public health; or
   iii. Employment protection, social security.

Acknowledgements

We would like to thank the following Deloitte professionals for their support and contribution to this publication:

Maanya Anand
Delhi

Faris Azimullah
Auckland

Ajay Bisht
Thane

Alex Cheung
Jakarta

Charlie Chye
Singapore

Abhishek Dubey
Auckland

Karen Grieve
Sydney

Ho Kyoo Hahn
Seoul

Hendro Hendro
Jakarta

Haruhito Kitano
Tokyo

Edith Lee
Hong Kong

Eric Leo
Sydney

Han Lin
Taipei

Max Lin
Taipei

Michelle Liu
Beijing

Toshiyuki Oba
Tokyo

Karthikeyan Palaniappan
Chennai

Rajesh Pradhan
Auckland

Roma Rudra
Thane

Piya Shedden
Melbourne

Ruby Shen
Beijing

Sowmya Vedarth
Bengaluru

Neeru Walia
Delhi

Frank Xiao
Beijing

Key contacts

Manish Sehgal
Asia Pacific Cyber Data & Privacy leader
+91 124 679 2723
masehgal@deloitte.com

Ian Blatchford
Asia Pacific Cyber leader
+61 2 9322 5735
iblatchford@deloitte.com.au

Australia

Daniella Kafouris
Partner
+61 3 9671 7658
dakafouris@deloitte.com.au

Chinese Mainland

Frank Tengfei Xiao
Partner
+86 10 8512 5858
frankxiao@deloitte.com.cn

Hong Kong SAR

Brad Lin
Partner
+852 2109 5353
bradlin@deloitte.com.hk

Japan

Haruhito Kitano
Partner
+81 80 3591 6426
haruhito.kitano@tohmatsu.co.jp

New Zealand

Faris Azimullah
Partner
+64 9303 0842
fazimullah@deloitte.co.nz

South Asia

Manish Sehgal
Partner
+91 124 679 2723
masehgal@deloitte.com

South Korea

Sung Kyu Cho
Director
+82 2 6676 2978
sungkcho@deloitte.com

Southeast Asia

Charlie Chye
Director
+65 6800 4580
cchye@deloitte.com

Taiwan

Max Y Lin
Partner
+886 (2) 2725 9988 (ext. 7779)
maxylin@deloitte.com.tw

Designed by CoRe Creative Services. RITM1233938

This is printed on environmentally friendly paper