



## **Centre for Regulatory Strategy Asia Pacific**

# **Safeguarding Data Privacy in AI:** Balancing Innovation against Risk, and Ethical Challenges



October 2025

# Navigating the Report

Click icon to navigate to the relevant section

Introduction		Key Data Privacy Challenges	
Overview of the Regulatory Landscape		Recommendations	

Jurisdictional Deep Dive	Australia		Indonesia		Philippines		Thailand	
	China (Mainland)		Japan		Singapore		Vietnam	
	Hong Kong SAR		Malaysia		South Korea			
	India		New Zealand		Taiwan (China)			

Contacts	
Endnotes	





# Introduction

**In the digital age, the intersection of data privacy and artificial intelligence (AI) has become a critical frontier for innovation and ethical consideration.**

AI technologies are advancing at an unprecedented pace and increasingly rely on vast amounts of personal information to function effectively, raising significant concerns about how personal information is collected, used, and protected.

AI technologies amplify longstanding privacy concerns that have existed throughout the era of widespread internet use and digital data gathering and storage. What sets AI apart is its vast appetite for data and the opacity of its processes, further diminishing user control over what personal information is gathered, how it is utilised, and the options available for modification or deletion. In today's digital landscape, individuals find it nearly impossible to avoid pervasive online tracking and the rise of AI has the potential to further exacerbate these challenges.

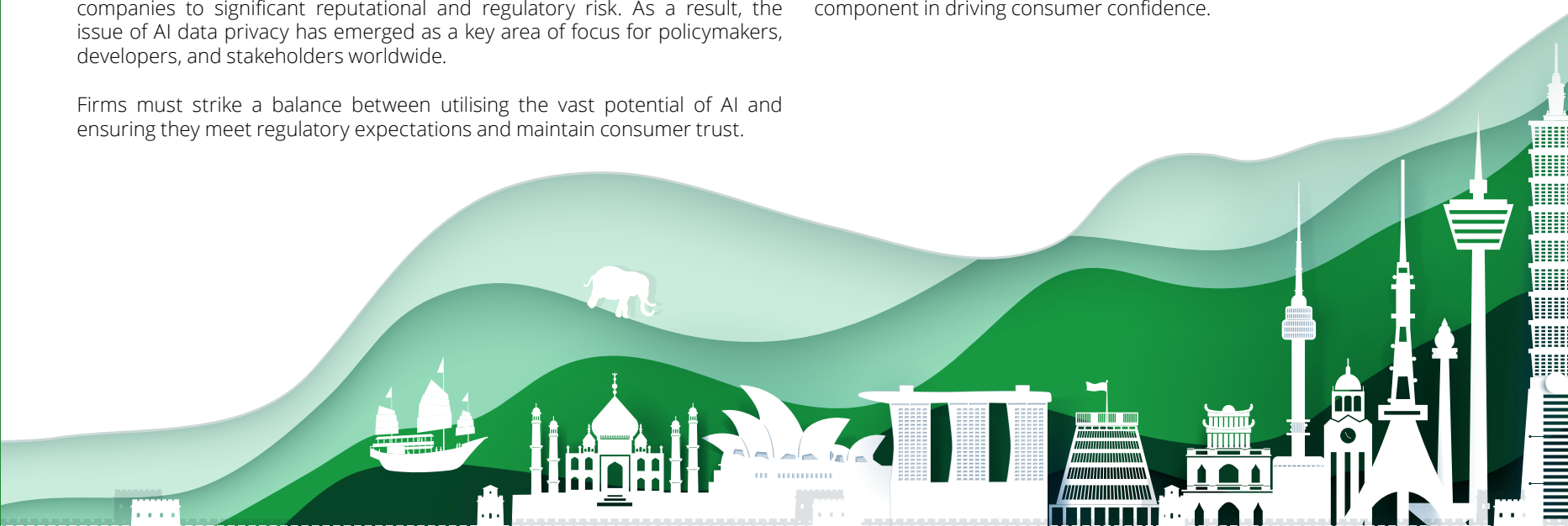
From conversational tools such as ChatGPT and smart home devices to advanced applications used for healthcare diagnostics and facial recognition, AI systems depend on data from both users and the broader population to refine models and produce results. However, without robust privacy protections, this data may be vulnerable to misuse or exploitation, potentially exposing companies to significant reputational and regulatory risk. As a result, the issue of AI data privacy has emerged as a key area of focus for policymakers, developers, and stakeholders worldwide.

Firms must strike a balance between utilising the vast potential of AI and ensuring they meet regulatory expectations and maintain consumer trust.

This report examines data privacy as an "AI-adjacent" regulatory issue and explores the challenges that emerge when the two domains converge.<sup>1</sup> We analyse the current data privacy landscape across the Asia Pacific (AP) region, along with specific data-related AI requirements, with the goal of providing clear insights and practical recommendations to help stakeholders navigate this evolving ecosystem responsibly and effectively.

## Consumer Concerns

Attitudes of consumers towards the security of their data is a key factor in the development of AI with significant reputational risk associated with a loss of consumer confidence.<sup>2</sup> Only half of consumers consider the benefits of online and digital services to outweigh data security risks.<sup>3</sup> The Deloitte "State of Ethics and Trust in Technology Annual Report" (Third Edition) found that 72% of technical professional and business respondents in the USA ranked data privacy as one of their top three concerns, with 40% of respondents ranking it as their top concern.<sup>4</sup> Further, 62% of consumers place higher trust in companies whose AI use they consider to be ethical, with 53% of consumers being willing to pay a premium for such products.<sup>5</sup> Meanwhile, among Australian consumers, the misuse of personal data by malicious actors and concerns regarding the privacy of personal information have emerged as two of the most significant issues associated with Generative AI (GenAI). Notably, 65% of survey respondents highlighted these matters as primary concerns.<sup>6</sup> Therefore, ensuring that AI data privacy is adequately addressed is an increasingly vital component in driving consumer confidence.



# Overview of the Regulatory Landscape

**A key development in data privacy regulation is the introduction of the General Data Protection Regulation (GDPR) in the European Union (EU).<sup>7</sup>**

The GDPR applies to any organisation handling EU residents' data, regardless of location, and enforces strict rules on data collection, use, and protection. Key features include robust data subject rights, stringent accountability requirements, and significant penalties for non-compliance, making it a leading global standard for data protection. The GDPR also introduces other rigorous requirements, such as keeping detailed records of data protection measures, promptly reporting data breaches to regulators, and designating a Data Protection Officer in certain cases. These obligations require organisations to establish, review, and demonstrate robust compliance processes, which adds to the overall complexity and cost of regulatory compliance.

The GDPR has been a pioneering regulation in the context of data privacy, with many AP regulators either introducing new data privacy regulations or updating existing frameworks following its introduction. Further, the GDPR is a prominent example of the “Brussels effect,” due to its significant extraterritorial impact, exposing a large number of producers and consumers of data-driven applications to EU regulation. Large international companies, therefore often find it more effective to adopt these rules across their global operations to enhance efficiency and interoperability. Whilst the GDPR does not specifically refer to AI, it puts in place several key requirements particularly relevant to firms utilising this technology.

The global landscape of data privacy and AI regulation is rapidly evolving, with significant steps taken across the AP region to enhance personal data protection. Australia, for example, has introduced the Privacy and Other Legislation Amendment Bill 2024 to address rising data breaches and enhance children's online privacy. Mainland China's (“China”) Personal Information Protection Law (PIPL) and Data Security Law (DSL) set comprehensive standards for data protection and national security. Singapore and Hong Kong have released detailed guidelines for AI, emphasising transparency and ethical considerations. Japan, South Korea, and Taiwan (China) (“Taiwan”) have updated their data privacy laws to include enhanced security measures and flexible data processing rules. India's Digital Personal Data Protection Act (DPDP) and DPDP Rules establish a robust framework for data protection and compliance.

Indonesia, Malaysia, the Philippines, and Vietnam are also strengthening their data protection laws to ensure international alignment and to address modern challenges. These efforts reflect a growing commitment to balance innovation with robust data protection and foster international collaboration. Furthermore, taken as a whole, most regimes include features that grant rights to individuals regarding their personal data and require data controllers and processors to safeguard and manage their data appropriately.

However, approaches to integrating AI specific considerations into data privacy regulatory frameworks vary significantly. Some jurisdictions with a high emphasis on fostering AI development, such as Hong Kong, Singapore, and South Korea have been proactive in releasing AI specific guidance in relation to their data privacy regulatory regimes. In contrast, other AP jurisdictions have focused on establishing and strengthening their general data privacy regulations and legislation. Although these frameworks do not specifically address the use of AI, firms deploying such technologies are still required to comply with the overarching regulatory requirements.

Furthermore, as is often the case, the devil lies in the details. Even when regulatory priorities are generally aligned, important differences may persist in specific consent requirements, breach notification timelines, and rules governing data storage and transfers. In some regions such as China, South Korea and Indonesia strict data localisation laws may clash with the widespread adoption of cloud hosting in others. AI models, which routinely ingest and process data from multiple sources, can quickly turn minor compliance gaps into significant legal risks. For instance, organisations may inadvertently store or reproduce personal data in locations where local regulations expressly forbid it. This is a problem that can be exacerbated by the use of third-party service providers for data storage purposes where oversight of the data location cannot be tracked by the principal firm.

Given the rapid pace of AI development over the last year, firms should expect local regulators to continue adapting their regulatory expectations in line with current global trends and technological advancements. Therefore, AP firms using AI must maintain a robust data privacy framework and ensure that proper governance and oversight are in place to prevent regulatory breaches and to handle personal data ethically and legally.





## Navigating the Data Privacy Landscape: Overview of AP Regional Requirements

		Enforcement & Penalties	Specific Data Guidelines/ Requirements for AI	Extraterritoriality	Cross-Border Data Rules	Data Protection Officer (DPO) Requirements	Data Localisation Rules*	Sensitive Personal Categories**	Child Data Protection Rules	Data Subject Rights
	Australia	✓	✓	✓	✓	✗	✗	✓	✓	✓
	China (Mainland)	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Hong Kong SAR	✓	✓	✗	✓	✗	✗	✓	✓	✓
	India	✓	✗	✓	✓	✓	✗	✗	✓	✓
	Indonesia	✓	✗	✓	✓	✓	✓	✓	✓	✓
	Japan	✓	✗	✓	✓	✗	✗	✓	✓	✓
	Malaysia	✓	✗	✓	✓	✓	✗	✓	✓	✓
	New Zealand	✓	✓	✓	✓	✓	✗	✓	✓	✓
	Philippines	✓	✓	✓	✓	✓	✗	✓	✓	✓
	Singapore	✓	✓	✓	✓	✓	✗	✓	✓	✓
	South Korea	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Taiwan (China)	✓	✗	✓	✓	✗	✗	✓	✓	✓
	Thailand	✓	✗	✓	✓	✓	✓	✓	✓	✓
	Vietnam	✓	✗	✓	✓	✓	✓	✓	✓	✓

\*Some regions such as Australia do not have an overarching data localisation rule, however, specific regulations for sectors such as healthcare create localised data sovereignty requirements.

\*\*Sensitive personal categories' include for example health, employment, education, criminal justice and personal finance etc.





## Extraterritoriality

One of the most significant developments in global data privacy regulation is the principle of extraterritoriality, wherein laws apply beyond a jurisdiction's borders. The EU's GDPR exemplifies this approach. Under Article 3 of the GDPR, the regulation applies not only to organisations established within the EU, but also to entities outside the EU if they offer goods or services to, or monitor the behaviour of, individuals within the EU. This means that a company in China, India, or anywhere else in the world must comply with the GDPR if it processes the personal data of EU residents, regardless of where the data processing physically occurs. This extraterritorial scope is designed to ensure that EU citizens' data is protected wherever it travels, reflecting the borderless nature of digital commerce and data flows.

The extraterritoriality principle is not unique to Europe; it is increasingly being adopted by data privacy regulators across the AP region. For instance, Singapore's Personal Data Protection Act (PDPA) can apply to organisations outside Singapore if they collect or process personal data in the course of offering goods or services to individuals in Singapore. Similarly, South Korea's Personal Information Protection Act (PIPA) and Japan's Act on the Protection of Personal Information (APPI) have provisions that may extend their reach to foreign entities handling their citizens' data. This growing trend reflects a global recognition that effective data privacy protections must transcend national boundaries. For multinational organisations, this means compliance efforts can no longer be limited to local laws; a comprehensive, cross-border approach to data privacy governance is now essential to meet the expectations of regulators around the world.



# Key Data Privacy Challenges



## Consent

Regulations requiring the lawful, fair, and transparent processing of personal data often centre around the concept of consent and are highly relevant to the use of AI. Organisations deploying AI must ensure that any personal data they collect and process is handled in accordance with a clearly defined legal basis, such as obtaining explicit consent from individuals. This is particularly significant for AI systems that may infer sensitive information or make automated decisions impacting individuals. To remain compliant, organisations must communicate clearly and openly on how customers' data will be managed, ensuring individuals are informed and able to exercise their right to have their data removed. Further, when obtaining consent organisations should be specific about how data will be used and should avoid broad, vague or bundled consent requests, particularly when dealing with sensitive information or AI use cases considered to be 'high-risk'. Robust safeguards should also be put in place to prevent information from being misused or repurposed for AI training beyond what was originally intended. Before using data for a new purpose, or following a change in the objectives or outputs of an AI system, organisations should evaluate whether such uses align with the initial disclosure. They must also maintain transparency with users and where appropriate reassess and renew user consent. Organisations should also ensure that third-party AI providers have robust mechanisms for capturing and managing data subjects' consent that aligns with data privacy obligations and stakeholder expectations. By embedding these principles into AI systems, organisations can reduce the risk of unlawful data use and demonstrate respect for individuals' privacy and autonomy.



## Cross-Border Data Transfers

Cross-border data transfer regulations are closely linked to AI usage as many AI systems rely on global data flows, often processing information across multiple regions. These regulations require organisations to ensure that personal data transferred outside their jurisdiction, especially to locations without equivalent privacy regulations, is adequately safeguarded. For AI applications, this requires firms to assess where their data is stored, processed, and accessed, and to enact safeguarding processes when exporting data. Furthermore, most regions differentiate between personal data and sensitive data (such as health, biometrics, or personal finance) and/or have stricter privacy requirements for minors. Therefore, the cross-border movement of these types of datasets is often subject to additional restrictions. Similarly, certain regions enforce data localisation requirements for particular types of sensitive data such as those related to health. These regulations should be thoroughly understood during the initial design of AI models and regularly reviewed after deployment. Non-compliance can lead to significant regulatory, legal, and reputational risks, as improper data transfers may violate privacy rights and regulatory requirements. By following cross-border data transfer regulations, organisations developing or deploying AI systems can protect individuals' privacy and ensure firm operations remain lawful in a global context.





## Data Minimisation

Data minimisation is a core aspect of data privacy regulation, with the GDPR defining it as personal data collection being “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed” (Article 5(1)(c)).<sup>8</sup> Furthermore, according to the storage limitation principle, companies should only retain personal data for as long as necessary to meet its objectives, after which it must be promptly deleted. Data minimisation regulations require organisations to collect and process only the personal data that is strictly necessary to achieve a specific, legitimate purpose. In the context of firms using AI, this principle is particularly important because AI systems often require large datasets for training and operation, which can increase the risk of unnecessary or excessive data collection. To comply with data minimisation regulations, firms using AI must carefully assess and justify the types and amounts of data they gather, ensuring that they do not collect irrelevant or excessive information. By adhering to data minimisation principles, organisations can build AI solutions that offer greater privacy protection and are less likely to infringe on individuals’ rights. In our view, AI models should be designed from the outset with a clear, specific goal in mind, ensuring that all data inputs are directly relevant and justifiable for that goal. Such an approach safeguards privacy, reduces risks, and enhances compliance with data protection regulations. However, this principle poses challenges for General-Purpose AI (GPAI) models, which are trained on vast, diverse datasets to achieve broad capabilities. Strict data minimisation would limit the scope and utility of GPAI models, as their effectiveness often relies on having access to large-scale, and granular data during training. Consequently, while data minimisation aligns well with narrowly focused AI systems, it is inherently less compatible with the open-ended nature of GPAI.





# Recommendations

Below are some key considerations for firms:



**Ensure** compliance-by-design by addressing current regulatory requirements and potential risks from the outset. AI systems must also be suitably flexible to adapt to new requirements



**Invest** in expertise and capacity within the firm to develop AI tools and functions in line with data privacy regulations and industry best practices



**Plan for retirement** by establishing policies, processes and controls for archiving and destroying AI data in order to ensure data is not kept longer than necessary and is disposed of appropriately when it is no longer required



**Raise awareness** within the firm of the importance of data privacy relating to AI use to create a culture of security around AI. Achieving this demands operational and cultural shifts to create effective collaboration across risk, legal, compliance, technology, and business teams



**Design** an AI data privacy strategy which focuses on a strong governance framework and embeds privacy-by-design into the AI lifecycle from data collection to model deployment including model re-training. Having a clearly defined purpose and outcome for each AI model or use case is also critical to minimising and protecting the use of personal data



**Strengthen** data privacy by anonymising training data, encrypting information both at rest and in transit, and managing the amount of data used by machine learning algorithms. Define clear ownership for data privacy oversight and decision making. Utilise real-time monitoring for suspicious activities and perform regular privacy risk assessments and audits to ensure compliance and security. Organisations should also ensure that third-party platforms or cloud services involved in AI processing adhere to their internal privacy obligations, including data sovereignty requirements, and provide full traceability of data access and usage





**Build trust** with consumers and key stakeholders by proactively addressing individuals' concerns on how their personal data is being used. Organisations should also publish publicly available reports detailing how data is collected, accessed, and stored for use in AI systems. In cases involving sensitive information, any security incidents or breaches resulting in data leaks must also be disclosed in a timely manner



**Perform** ongoing monitoring to ensure AI systems remain compliant against future data privacy regulations. Regularly review models, datasets and processes for new privacy risks. Firms should also maintain detailed logs of data access and AI model usage to support auditability and accountability, enabling the organisation to demonstrate compliance with privacy regulations



**Engage** with experts on elements of AI governance design to make sure that you create a comprehensive and compliant AI framework within your firm. Deloitte's [Trustworthy AI Framework](#) offers a suite of services that combines advanced technological capabilities with leading governance practices to help you effectively guide your AI

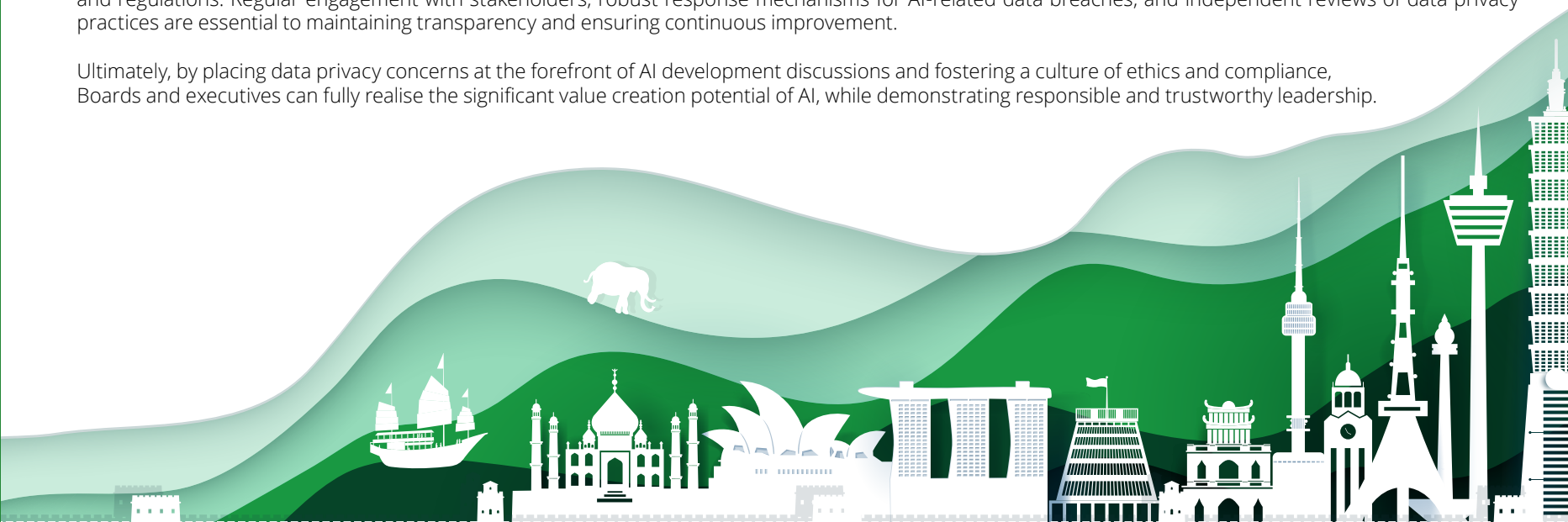


**Conduct** an assessment of the benefits of using a third-party service provider or investing in onsite data storage solutions. Rising costs and regulatory concerns relating to data transfers need to be considered when planning for data storage solutions in the future. For AI training datasets or inference pipelines that rely on multi-region data, this should also include a thorough transfer impact assessment (TIA)

In conclusion, Boards and company executives should champion a unified AI strategy in which data privacy is embedded as a core design principle, rather than treated as a mere compliance afterthought. This approach enables safe innovation, maintains stakeholder trust, and mitigates both reputational and regulatory risks.

Effective oversight of AI systems requires Boards and executives to set clear organisational expectations and accountability for data privacy. This includes aligning AI initiatives with overall risk management strategies, investing in necessary talent and resources, and staying informed about evolving technologies and regulations. Regular engagement with stakeholders, robust response mechanisms for AI-related data breaches, and independent reviews of data privacy practices are essential to maintaining transparency and ensuring continuous improvement.

Ultimately, by placing data privacy concerns at the forefront of AI development discussions and fostering a culture of ethics and compliance, Boards and executives can fully realise the significant value creation potential of AI, while demonstrating responsible and trustworthy leadership.



# Jurisdictional Deep Dive

There are clear contrasts in the approach and maturity of AI data privacy regulations across jurisdictions. However, data privacy regulations issued by AP jurisdictions converge around several key principles which broadly align with international regulatory standards such as the EU's GDPR. These include establishing the rights of data subjects, implementing data principles such as minimisation and purpose limitation, and mandating controls for cross-border data transfers.

The following section provides a deep dive into the current state of data privacy regulation across the region and how they intersect with the emergence of AI and AI specific requirements.

[Introduction](#)[Overview](#)[Key Data Privacy](#)[Recommendations](#)[Jurisdictional Deep Dive](#)[Australia](#)[China \(Mainland\)](#)[Hong Kong SAR](#)[India](#)[Indonesia](#)[Japan](#)[Malaysia](#)[New Zealand](#)[Philippines](#)[Singapore](#)[South Korea](#)[Taiwan \(China\)](#)[Thailand](#)[Vietnam](#)[Contacts](#)[Endnotes](#)








# Australia

## Data privacy is becoming an increasingly prominent topic within Australia.

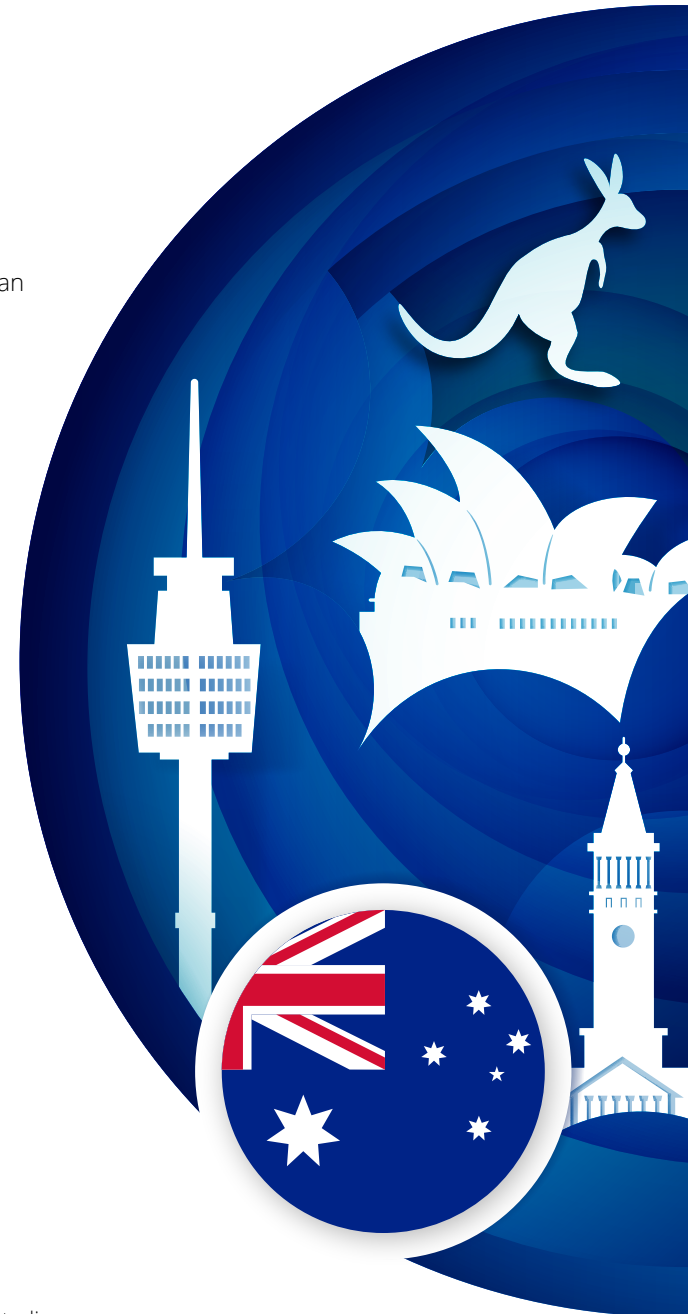
In May 2025, the Australian Office of the Australian Privacy Commissioner (OAIC)\* announced that businesses and government agencies reported more than 1,100 data breaches in 2024, the highest year on record and a 25% increase from 2023.<sup>9</sup> Phishing and social engineering/impersonation were cited as prominent methods by which data was stolen, while health service providers and the Australian Government notified of data breaches most frequently.

The Australian Government has prioritised the enhancement of data privacy regulations through the introduction of the *Privacy and Other Legislation Amendment Bill 2024* ("the Bill") which received royal assent on 10 December 2024.<sup>10</sup> The Bill forms part of the wider data privacy framework update following the introduction of the *Privacy Act 1988*<sup>11</sup>, updating data privacy regulations and the Australian Privacy Principles (APPs)<sup>12</sup> in line with modern demands.

### Key features of the Bill include:

-  Criminalisation of doxxing
-  Prohibition on serious invasions of privacy
-  Enhancement of policies relating to automated decision-making (ADM) systems
-  Establishment of a mandatory Children's Online Privacy Code by the OAIC
-  Providing protections for overseas disclosures of personal information

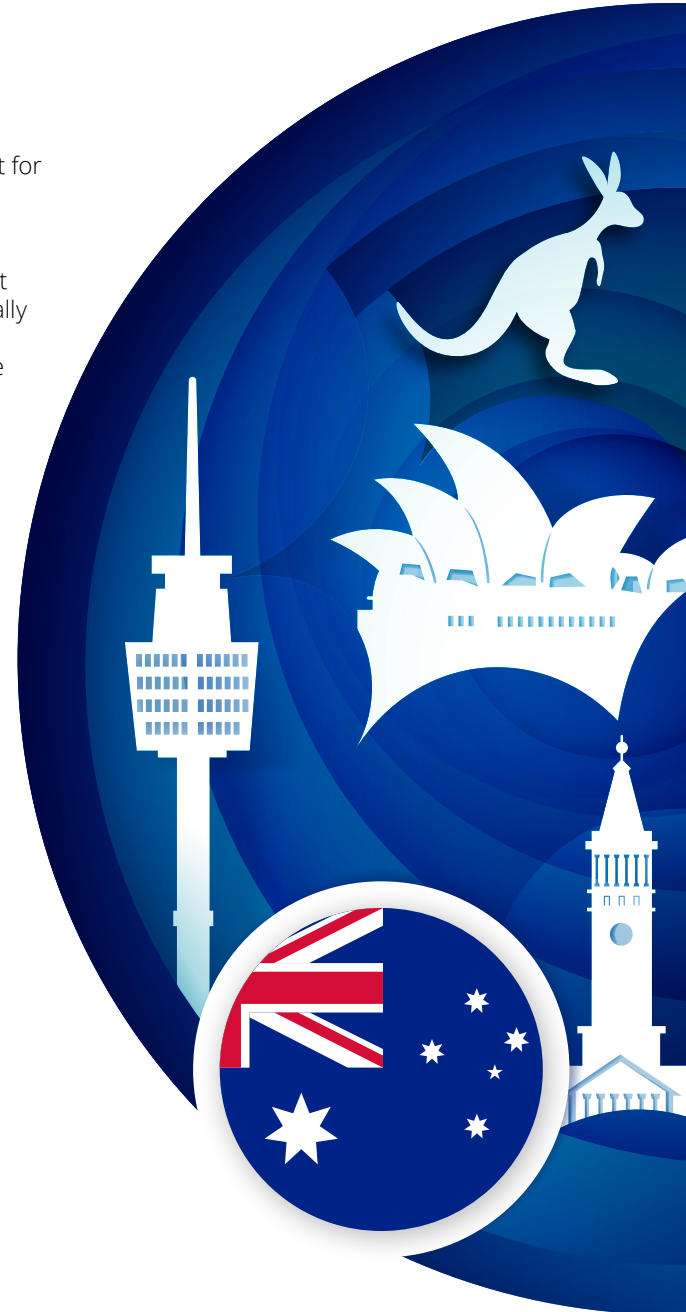
\*The OAIC is the government agency which regulates data privacy and enforces the data privacy legislation in Australia

[Introduction](#)[Overview](#)[Key Data Privacy](#)[Recommendations](#)[Jurisdictional Deep Dive](#)[Australia](#)[China \(Mainland\)](#)[Hong Kong SAR](#)[India](#)[Indonesia](#)[Japan](#)[Malaysia](#)[New Zealand](#)[Philippines](#)[Singapore](#)[South Korea](#)[Taiwan \(China\)](#)[Thailand](#)[Vietnam](#)[Contacts](#)[Endnotes](#)

A subsequent tranche of reforms is expected to be passed by the Australian government to further enhance data privacy regulations, however at the time of writing there has been no official timeline set for the release of these reforms.

Regarding AI, the OAIC has publicly identified the risks that AI poses in relation to data privacy and protection. In October 2024, the OAIC released two guides detailing how the Bill applies to AI. The first guide will make it easier for businesses to comply with their privacy obligations when using commercially available AI products and help them to select an appropriate product<sup>13</sup>, whereas the second provides privacy guidance to developers using personal information to train generative AI models.<sup>14</sup> The release of these guides will enable Australian firms to establish proper data governance processes to ensure that AI innovation is conducted in compliance with data privacy regulations.

Furthermore, in February 2025 the Australian Privacy Commissioner signed a joint declaration with data protection authorities from South Korea, France, the UK, and Ireland at the AI Action Summit in Paris, committing to establish data governance that enables “privacy-protective AI”.<sup>15</sup> By doing so, Australia signaled its commitment to global collaboration in establishing effective governance frameworks for enhancing data privacy protections for AI while continuing to foster innovation.



Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia



China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



# China (Mainland)

**Mainland China ("China") has been an active jurisdiction in establishing its data privacy and data security framework in recent years.**

The *Personal Information Protection Law* (PIPL), enacted in November 2021, is China's first dedicated legislation for personal information protection.<sup>16</sup> It governs the processing of personal data and safeguards individual rights, emphasising principles like legality, transparency, and necessity.

## **Key provisions include:**



### **Individual Rights**

People can access, correct, and request deletion of their data. They can also request data transfers to other processors



### **Minors' Data**

Consent from parents or guardians is required for processing data of minors under 14, along with specific processing rules



### **Automated Decision-Making**

The law prohibits unreasonable differential treatment in trade practices and mandates opt-out options for targeted marketing



### **Data Transfers**

Personal information can only be transferred outside Mainland China with explicit consent and compliance with security assessments or contracts



### **Extraterritoriality**

Foreign organisations processing data of individuals in China must comply with the PIPL and designate representatives in China



### **Enforcement**

Violations can result in fines up to RMB 50 million or 5% of annual turnover, and potential business operation suspensions

[Introduction](#)[Overview](#)[Key Data Privacy](#)[Recommendations](#)[Jurisdictional Deep Dive](#)[Australia](#)[China \(Mainland\)](#)[Hong Kong SAR](#)[India](#)[Indonesia](#)[Japan](#)[Malaysia](#)[New Zealand](#)[Philippines](#)[Singapore](#)[South Korea](#)[Taiwan \(China\)](#)[Thailand](#)[Vietnam](#)[Contacts](#)[Endnotes](#)



The *Data Security Law* (DSL) was enacted on 1 September 2021, it establishes a comprehensive framework for data management and protection in China.<sup>17</sup>

**Key features of the DSL include:**



**National Security Focus**

The law emphasises the importance of data security for national security and public interest, outlining responsibilities for data handlers to prevent risks



**Accountability and Penalties**

Organisations that violate the DSL can face strict penalties, including fines and operational suspensions, reinforcing the importance of compliance



**Coordination Among Authorities**

The law mandates cooperation between various governmental bodies to oversee data security and ensure compliance across sectors



**Data Handling Obligations**

Entities that handle data must implement security measures to protect it from breaches and misuse. This includes risk assessments and incident response mechanisms



**Cross-Border Data Transfers**

The DSL sets conditions for transferring data outside China, including security assessments and compliance with national laws. Permissible transfers include those passing a government security assessment and those which have gained explicit consent from the data subject



**Data Classification**

The DSL categorises data into different levels based on its importance to national security, economic stability, and public interest, requiring tailored security measures for each category. Core Data includes data which is important to national security, Important Data is deemed to be less sensitive than Core Data but still important to national and economic security, and General Data is data which would not cause major harm if leaked



Introduction

Overview

Key Data Privacy

Recommendations

**Jurisdictional Deep Dive**

Australia

**China (Mainland)**



Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



The Cyberspace Administration of China (CAC) oversees compliance and management of personal information protection. The CAC is the primary regulator which oversees the enforcement of the PIPL and the DSL. The PIPL and DSL do not have specific guidance for financial services firms, however the regulations governing the management of personal data, cross-border data transfers, and enhanced security requirements for sensitive data are directly applicable to financial institutions.

In relation to AI, the PIPL's regulation of Automated Decision-Making is directly applicable to AI applications. The PIPL requires transparency, fairness, and the right to opt-out of applications which use Automated Decision-Making, and firms using AI applications must comply with these requirements. The DSL does not have specific AI regulations, however, its guidance around handling large and sensitive datasets must be adhered to by firms using AI applications.

In relation to financial services specifically, the National Financial Regulatory Administration (NFRA) introduced the *Administrative Measures for Data Security of Banking and Insurance Institutions* ("NFRA Data Rules") in December 2024.<sup>18</sup>

#### Key features of the NFRA Data Rules include:



The rules apply to designated entities, including commercial banks, trust companies, and insurance firms, as well as other financial organisations



Data is classified into four categories - customer data, business data, operational and management data, and system operation/security data, with levels of core, important, sensitive, and general data



"Important data", which poses risks to national security or public safety is subject to stricter regulations



Major requirements include establishing governance structures, integrating data security into risk management, registering data assets, and complying with outsourcing regulations



A baseline for data security protection outlines minimum standards for data management



Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)



Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes





Institutions must conduct security assessments for sensitive data, monitor threats, and establish incident response mechanisms, including timely reporting of incidents



Comprehensive data security audits are required at least every three years

China introduced its first regulatory policy for the GenAI industry, the 'Interim Measures for the Management of Generative Artificial Intelligence Services,' ("the Measures") effective 15 August 2023.<sup>19</sup> Developed by the CAC, the measures aim to standardise the industry and encourage innovation.

#### Key points include:



##### Regulatory Framework

Establishes legal responsibilities for service providers regarding data compliance and intellectual property



##### Supervision

Outlines guidelines for compliance and oversight, including assessment and record-filing for AI services



##### International Regulations

Requires overseas providers to comply with Chinese laws to mitigate risks



##### Data Quality

Providers must ensure training data is high-quality, accurate, diverse, and legally sourced, with user consent required for any personal information used

Through the Measures China has mandated that AI applications and service providers must comply with the existing data protection laws as well as providing additional guidance relating to data quality and consent.



Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)



Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



# Hong Kong SAR

Data privacy in Hong Kong SAR ("Hong Kong") comes under the jurisdiction of the Office of the Privacy Commissioner for Personal Data (PCPD).

The data privacy legislation in Hong Kong, the *Personal Data (Privacy) Ordinance* (PDPO), is one of the longest standing data privacy laws in the AP region.<sup>20</sup> The most recent amendments to the PDPO were made in 2021 and focused on data breach notifications, data retention policies, direct marketing regulations, and increased enforcement powers for the PCPD.<sup>21</sup>

In June 2024, the PCPD released specific guidance for data privacy relating to the use of AI: *Artificial Intelligence: Model Personal Data Protection Framework (Model Framework)*.<sup>22</sup> This built upon a previous guidance note issued in 2021 *Guidance on the Ethical Development and Use of Artificial Intelligence*.<sup>23</sup>

## Key points included:



### Target Audience

The Model Framework is designed for all organisations using AI systems with personal data, expanding beyond the original focus on AI developers



### Risk-Based Approach

It aligns with the PCPD's earlier recommendations and provides practical guidance for compliance with the Personal Data (Privacy) Ordinance (PDPO)



### Core Values and Principles

The framework emphasises three data stewardship values (Respectful, Beneficial, Fair) and seven ethical principles (Accountability, Human Oversight, Transparency, Data Privacy, Beneficial AI, Reliability, Fairness)



### Framework Structure (comprising four parts)

AI Strategy and Governance, Risk Assessment and Human Oversight, Customisation of AI Models and Implementation, and Stakeholder Communication. The update reflects commercial realities by focusing on the customisation and management of AI systems

Overall, the Model Framework aims to help organisations navigate the complexities of AI while ensuring data protection and ethical considerations.

[Introduction](#)[Overview](#)[Key Data Privacy](#)[Recommendations](#)[Jurisdictional Deep Dive](#)[Australia](#)[China \(Mainland\)](#)[Hong Kong SAR](#)[India](#)[Indonesia](#)[Japan](#)[Malaysia](#)[New Zealand](#)[Philippines](#)[Singapore](#)[South Korea](#)[Taiwan \(China\)](#)[Thailand](#)[Vietnam](#)[Contacts](#)[Endnotes](#)

# India

## India passed major legislation recently in relation to data privacy and protection.

India passed major legislation recently in relation to data privacy and protection. The *Digital Personal Data Protection Act, 2023* (DPDP Act) establishes a comprehensive framework for data protection in India.<sup>24</sup>

### Key features include:



#### Establishment of the Data Protection Board of India (DPB)

An independent body to address disputes relating to data privacy violations



#### Consent

Explicit consent is required for data processing, with rights to withdraw consent



#### Individual Rights

Rights to access, correct, and erase personal data



#### Breach Notification

Mandatory notification in case of data breaches



#### Penalties

Significant penalties for non-compliance



#### Exemptions

Certain exemptions for government agencies



#### Processing Principles

Data must be collected for specified purposes, minimised, and retained only as necessary



#### Cross-Border Transfers

Data can be transferred outside India with safeguards (e.g., transferring data to a country with the same level of data protection regulations and attaining explicit consent)

[Introduction](#)[Overview](#)[Key Data Privacy](#)[Recommendations](#)[Jurisdictional Deep Dive](#)[Australia](#)[China \(Mainland\)](#)[Hong Kong SAR](#)[India](#)[Indonesia](#)[Japan](#)[Malaysia](#)[New Zealand](#)[Philippines](#)[Singapore](#)[South Korea](#)[Taiwan \(China\)](#)[Thailand](#)[Vietnam](#)[Contacts](#)[Endnotes](#)



In January 2025, the Indian Ministry of Electronics and Information Technology released the *Draft Digital Personal Data Protection Rules* (DPDP Rules) which are designed to operationalise the DPDP Act.<sup>25</sup> The public consultation ended in March 2025, and the rules are set to be implemented through publishing in the Gazette by the end of the year.

**Key features of the DPDP Rules include:**



Individuals can access, correct, and erase their data, with mechanisms to withdraw consent and handle complaints effectively



Data fiduciaries ensure privacy and security through defined retention timelines, compliance audits, and transparent processes



Regulatory rules mandate encryption, breach reporting within 72 hours, and robust identity verification, with special protections for children and those with disabilities

Neither the DPDP Act nor the DPDP Rules contain specific provisions for data privacy regulations relating to AI. However, the DPDP Act and Rules establish a framework which promotes ethical data handling, which remains a key issue for firms establishing a AI governance approach.



Introduction

Overview

Key Data Privacy

Recommendations

**Jurisdictional Deep Dive**

Australia

China (Mainland)

Hong Kong SAR

**India**



Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



# Indonesia

**Indonesia Law No. 27 of 2022, commonly referred to as the Personal Data Protection Law (PDP Law), is Indonesia's first comprehensive law dedicated to the protection of personal data.**

It became effective in October 2022.<sup>26</sup>

## *Key features of the PDP Law include:*



Violations lead to fines or criminal penalties



**Covers all entities processing Indonesians' personal data**, within or outside Indonesia



**Gives individuals rights** - access, correct, delete, withdraw consent, object, restrict, and complain



Requires controllers/processors to process data lawfully, protect data, issue a notification for breaches, and appoint a data protection officer if needed



**Consent is a primary ground for processing**, but the Law also recognises other bases such as contractual necessity, legal obligations, vital interests, public interest, and legitimate interests



Cross-border transfers are allowed with to jurisdictions with an equal or higher level of data protection than Indonesia, and/or if an adequate level of binding data protection is available for the specific transfer



**Mandates the creation of a personal data protection authority** to enforce the PDP Law (this as not yet been created at the time of publishing). Ministry of Communication and Digital will oversee compliance in the interim period

The two-year transition period concluded in October 2024, and all in-scope entities are now required to fully comply with the PDP Law. In-scope entities include any parties processing the personal data of Indonesian citizens or residents, whether operating within Indonesia or overseas.



Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia



Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



# Japan

The core data privacy regulation in Japan is the *Act on the Protection of Personal Information (APPI)* which is overseen by the *Personal Information Protection Commission Japan (PPC)*.

The APPI regulates data handling, cross-border data transfers, and the protection of personal information in Japan.<sup>27</sup> The PPC is required to review the APPI every three years to ensure it is suitable for current industry trends. In June 2024, the PPC released the Interim Report on Considerations for the *Triennial Review of the Act on Protection of Personal Information* ("Interim Report") with proposed amendments to the APPI released for public consultation.<sup>28</sup> The amended APPI is expected to be published in 2025.

## Key features of the current APPI include:



### Definition of Personal Information

Covers any information that can identify a living individual, including "personal data" (organised information) and "Sensitive personal information"



### Data Subject Rights

Individuals can access, correct, request deletion or object to data processing of their data



### Security Measures

Businesses must implement necessary measures to prevent leaks, loss, or damage of personal data



### Data Breach Notification

Notification is mandated to the PPC and affected individuals if there is a risk of harm



### Outsourcing

Requires appropriate supervision of contractors when outsourcing data processing



### Principles of Data Processing

Requires collection and use of personal information only for clear, specified, and legitimate purposes. Prohibition on using data beyond the stated purpose needs additional consent

[Introduction](#)[Overview](#)[Key Data Privacy](#)[Recommendations](#)[Jurisdictional Deep Dive](#)[Australia](#)[China \(Mainland\)](#)[Hong Kong SAR](#)[India](#)[Indonesia](#)[Japan](#)[Malaysia](#)[New Zealand](#)[Philippines](#)[Singapore](#)[South Korea](#)[Taiwan \(China\)](#)[Thailand](#)[Vietnam](#)[Contacts](#)[Endnotes](#)



### Consent Requirements

Prior consent is needed for collecting sensitive information, for providing personal information for a third party, and for cross-border data transfers (with some exceptions). Individuals must be informed about the purpose of use



### Cross-Border Data Transfers

Transferring data outside of Japan calls for one of the following conditions:

- The recipient country is recognised to have an adequate level of protection
- Relevant safeguards are in place
- Individual consent is obtained



The Interim Report that will be the basis of the APPI amendment in 2025 makes a number of data privacy proposals which will impact firms using AI in their business operations. Some of the proposals include rules on the proper handling of personal information, including biometric data and the data of minors



**Enhanced monitoring** and supervision for compliance with the APPI, including fines and criminal penalties for non-compliance



The **ability to use personal data without obtaining individual consent** to train AI models in some instances (subject to restrictions and limitations).



**Restrictions on providing information to third parties** and 'opt-out' provisions



Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan



Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



The PPC also published a "Precautionary Notice on Use of Generative AI Services" In June 2023.<sup>29</sup> The notice outlines several key requirements for entities handling personal data:



#### **Purpose Limitation**

Entities should enter personal information into generative AI services only to the extent necessary to achieve the specific purpose of use



#### **Prohibition on Machine Learning use**

Entities must ensure that personal data entered into generative AI services is not used for machine learning purposes by the AI service provider



#### **Secondary Use Restrictions**

The PPC cautions that use personal data for secondary purposes, such as training AI systems, could constitute a breach of the APPI

Additionally, the precautionary notice includes specific instructions directed at OpenAI, the provider of the ChatGPT service, to ensure compliance with these requirements.



Introduction

Overview

Key Data Privacy

Recommendations

**Jurisdictional Deep Dive**

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

**Japan**



Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes





# Malaysia

Malaysia passed the **Personal Data Protection Act (PDPA)** in June 2010, and it became effective in November 2013.<sup>30</sup>

The PDPA enabled the creation the Personal Data Protection Department (JPDP) in May 2011 as the government agency to oversee the PDPA. The PDPA has acted as the foundation for data privacy legislation in Indonesia since its inception.

## Scope

Applies to commercial transactions involving personal data in Malaysia; excludes government data and data processed outside Malaysia unless intended for local processing.

*The PDPA is constructed around 7 key principles:*



Lawful processing with **consent**



**Individuals informed** about data collection with the option to decline



Data disclosed only for consented purposes, unless permitted by law



**Adequate security** measures must be in place



**Data retention limited** to necessity



**Data accuracy**, completeness, and currency must be ensured



Individuals have the **right to access and correct** their data



Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia 

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



In October 2024, the Malaysian government released the *Personal Data Protection (Amendment) Act 2024* (PDPA) which updates provisions included in the PDPA and enhances alignment to international data protection standards.<sup>31</sup>

#### Key updates include:



Terminology updates - "Data user" replaced with "data controller"; data processors now subject to security obligations



Biometric data classified as sensitive personal data, requiring specific handling and consent procedures



Mandatory data breach notification to PDPA and affected data subjects



Increased penalties - fines up to RM1,000,000 and/or imprisonment up to three years



Data subjects can request data in portable format



Whitelisting regime for cross-border data transfers removed; transfers allowed to countries with similar laws or equivalent protection



Data controllers and processors must appoint a Data Protection Officer (DPO)



Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia



New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



# New Zealand

In New Zealand, the key data privacy legislation is the *Privacy Act 2020* ("the Act").<sup>32</sup>

The Act is enforced by the Office of the Privacy Commissioner (OPC) and establishes 13 Information Privacy Principles (IPPs).

**These principles are:**



## **Purpose of Collection**

Information must be collected for a lawful purpose that is directly related to the agency's functions



## **Source of Information**

Personal information should be collected directly from the individual concerned, unless certain exceptions apply



## **Consent**

Individuals must be informed about the collection of their information and consent to it



## **Manner of Collection**

Information should be collected in a fair and lawful way, avoiding any unfair or misleading practices



## **Storage and Security**

Agencies must ensure personal information is stored securely and protected against loss, misuse, or unauthorised access



## **Access and Correction**

Individuals have the right to access their personal information and request corrections if it is inaccurate



## **Retention**

Personal information should not be kept for longer than necessary for the purpose for which it was collected



## **Disclosure**

Information should not be disclosed to third parties unless authorised by the individual or required by law



## **Use of Information**

Personal information should only be used for the purpose it was collected, unless consent is obtained for other uses



Introduction

Overview

Key Data Privacy

Recommendations

**Jurisdictional Deep Dive**

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

**New Zealand**

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes





### Accuracy

Agencies must take reasonable steps to ensure that personal information is accurate, up-to-date, and complete



### Transparency

Individuals should be informed about the use of their personal information and any related rights



### Cross-border Disclosure

Personal information should not be disclosed to overseas entities unless adequate protections are in place



### Unique Identifiers

Agencies should avoid assigning unique identifiers to individuals unless necessary for their functions

In terms of AI-specific data privacy guidance, the NPC has published guidance on how New Zealand firms might consider the IPPs when using AI.<sup>33</sup> The guidance suggests that AI-specific questions can be integrated into a Privacy Impact Assessment in alignment with the IPPs. It should be noted that this guidance is voluntary.



Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)


Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand 

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



# Philippines

The *Data Privacy Act 2012 (DPA)* was enacted in the Philippines in August 2012 to protect personal information and balance data flow with privacy rights.<sup>34</sup>

*Key elements of the DPA are:*



## Protection of Personal Information

Applies to both public and private entities processing personal and sensitive data



## Ensures Lawful Processing

Requires data to be processed lawfully, fairly, and transparently with specified purposes



## Grants Data Subject Rights

Includes rights to be informed, object, access, rectify, erase, and seek damages



## Mandates Security Measures

Requires appropriate security to protect data from unauthorised access and breaches



## Enforces Compliance

The National Privacy Commission (NPC) enforces the DPA with penalties for violations



## Allows Cross-Border Transfers

Permits data transfers to countries with adequate data protection laws



## Exempts Certain Activities

Exempts data processing only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned for public access to information of public concern, journalistic, artistic, literary, or research purposes intended for a public benefit, law enforcement and regulatory functions



Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines 

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes





The NPC has regularly released additional guidance to the DPA, issuing sector-specific guidance for the insurance industry,<sup>35</sup> as well as guidelines on specific topics such as data breach reporting and data sharing. The NPC also released specific guidance on the application of the DPA to AI systems.<sup>36</sup>

**Key features of the guidance on the application of the DPA to AI systems include:**



**Transparency and Communication**

Inform data subjects about the nature and purpose of data processing in AI, ensuring information is accessible and understandable



**Governance and Ethical Processing**

Implement effective governance mechanisms for ethical data processing, including monitoring for biases and allowing human intervention in automated decisions



**Data Accuracy and Minimisation**

Maintain accurate and up-to-date personal data while excluding unnecessary data that does not enhance AI development



**Interpretation of Rights**

Interpret regulations in a manner that favours the rights and interests of data subjects



**Obligations of Personal Information Controllers (PICs) and Personal Information Processors (PIPs)**

Adhere to privacy principles, implement security measures, and remain accountable for AI processing of personal data



**Legal Basis and Data Subject Rights**

Identify appropriate lawful bases for processing personal data and implement mechanisms to facilitate the exercise of data subject rights, ensuring accessibility throughout the AI system lifecycle



Introduction

Overview

Key Data Privacy

Recommendations

**Jurisdictional Deep Dive**

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

**Philippines** 

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



# Singapore

**The Singapore government has been proactive in establishing effective data governance in relation to the emergence of AI technology.**

The foundational data privacy legislation is the the *Personal Data Protection Act 2012* (PDPA).<sup>37</sup> In 2020, the Singapore government released the *Personal Data Protection (Amendment) Act 2020* which enhanced data privacy measures relating to consent, exceptions for data use, and new definitions.<sup>38</sup>

The Personal Data Protection Commission (PDPC) is the body responsible for enforcing the PDPA. It released the *Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems* ("the Guideline") in March 2024.<sup>39</sup>

The Guideline provides clarity on using personal data for machine learning under the PDPA.

## Key details include:



**Organisations can avoid obtaining consent by using business improvement or research exceptions** when training AI systems.

- The business improvement exception allows data use for understanding individual behaviour and enhancing or developing products and services. Restrictions include a prohibition on the use data to make decisions affecting the individual, and the data use must not have an adverse effect on the individual
- The research purpose exception supports broader research and development activities. The data must be used solely for research, and the research must be in the public interest or have clear societal benefits



Organisations are encouraged to anonymise personal data to protect privacy and limit the volume of data used for training



They **must be transparent about how they use personal data** in AI systems



Adherence to PDPA obligations such as consent, notification, and accountability is critical

[Introduction](#)[Overview](#)[Key Data Privacy](#)[Recommendations](#)[Jurisdictional Deep Dive](#)[Australia](#)[China \(Mainland\)](#)[Hong Kong SAR](#)[India](#)[Indonesia](#)[Japan](#)[Malaysia](#)[New Zealand](#)[Philippines](#)[Singapore](#)[South Korea](#)[Taiwan \(China\)](#)[Thailand](#)[Vietnam](#)[Contacts](#)[Endnotes](#)

### Other general regulations under the PDPA and associated amendments include:



#### Consent Requirement

Organisations must obtain consent from individuals before collecting, using, or disclosing their personal data



#### Purpose Limitation

Data can only be collected for specific, legitimate purposes that are communicated to individuals



#### Access and Correction Rights

Individuals have the right to access their personal data held by organisations and request corrections if necessary



#### Data Protection Obligations

Organisations must implement reasonable security measures to protect personal data and ensure its accuracy



#### Data Breach Notification

Organisations must notify affected individuals and the Personal Data Protection Commission (PDPC) in case of a data breach

The Infocomm Media Development Authority (IMDA) has also expanded its Privacy Enhancing Technologies (PETs) Sandbox to examine how PETs can facilitate greater access to data for generative AI applications while mitigating data protection risks.<sup>40</sup> Although the PDPC primarily handles data privacy, the IMDA also contributes to discussions and developments related to data governance and digital trust.

The PDPC has released the Proposed Guide to Synthetic Data (SD) Generation to establish a comprehensive framework for businesses employing SD generation as a PET.<sup>41</sup> This guide discusses the generation of synthetic data to train AI models. While typically fictitious and not deemed personal data, synthetic data poses re-identification risks. The guide recommends best practices for organisations to minimise these risks, tailored to common use cases, and outlines governance controls, contractual processes, and technical measures to address residual risks.



# South Korea

In 2011, Korea introduced the *Personal Information Protection Act (PIPA)* to establish the regulatory framework for personal data protection.<sup>42</sup>

The Personal Information Protection Commission (PIPC) is an independent data protection authority which formulates policies related to data privacy and supervises the application of the PIPA.

## Key features include:



### Consent

Requires explicit consent for data collection and processing



### Data Minimisation

Organisations must collect only necessary data



### Individual Rights

Individuals can access, correct, and delete their data



### Data Security

Mandates security measures to protect personal data



### Breach Notification

Organisations must notify individuals and the PIPC of data breaches



### Penalties

Imposes fines and sanctions for non-compliance



### Cross-Border Transfers

Regulates the transfer of data outside South Korea



### Supervision

Establishes the Personal Information Protection Commission to oversee compliance

[Introduction](#)[Overview](#)[Key Data Privacy](#)[Recommendations](#)[Jurisdictional Deep Dive](#)[Australia](#)[China \(Mainland\)](#)[Hong Kong SAR](#)[India](#)[Indonesia](#)[Japan](#)[Malaysia](#)[New Zealand](#)[Philippines](#)[Singapore](#)[South Korea](#)[Taiwan \(China\)](#)[Thailand](#)[Vietnam](#)[Contacts](#)[Endnotes](#)

In 2023, the PIPC underwent a review of the PIPA and introduced a revised version effective 15 September 2025.<sup>43</sup>

**Key revisions include:**



**Increased flexibility** for urgent data processing in emergencies



**Improved dispute resolution** processes for public and private entities



**Enhanced security measures** for public institutions handling large datasets



**Extended payment options** for small businesses facing administrative fines



**Guidelines for lawful data processing** via devices like drones without prior consent



Consistent regulations for online and offline entities regarding data breaches and child consent



Diverse conditions for international data transfers and revised penalty calculations



Introduction

Overview

Key Data Privacy

Recommendations

**Jurisdictional Deep Dive**

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

**South Korea**



Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes





The revised PIPA was introduced with AI in mind. Enhanced consumer data rights and conditions on international data transfers are initiatives from the PIPC to ensure the safe development of AI in Korea whilst ensuring the data privacy rights of individuals.

Furthermore, the PIPC, has introduced several detailed guidelines for GenAI relating to data privacy. These guidelines establish legal safety standards for the development, training, deployment, and governance of both commercial and internally developed AI systems.

The most recent and comprehensive of which is the August 2025 Guidelines for Personal Information Processing in the Development and Use of Generative Artificial Intelligence.<sup>44</sup>

The guidelines set out minimum standards for organisations at every stage of AI development and deployment. They apply comprehensively to all types of AI systems, including commercial large language models, fine-tuned open-source models, and fully self-developed solutions. For each category, the guidelines specify clear compliance obligations such as provider verification, robust data governance, thorough documentation, and privacy impact assessments. Notably, the guidelines also set out expectations for data sharing and service level agreement privacy clauses in the context of commercial API-based large language models.

***The compliance requirements across the AI lifecycle include:***



**Purpose Setting and Strategic Planning**

Defining objectives, assessing risks, and documenting the legal bases for data use



**Strategy Development and Architecture Design**

Implementing privacy-by-design, minimising data use, and ensuring compliance for cross-border transfers



**AI Training and Development**

Validating training data, ensuring fairness, and documenting safety measures



**Deployment and Management**

Ongoing monitoring, user consent management, incident response, and regular compliance reviews



Introduction

Overview

Key Data Privacy

Recommendations

**Jurisdictional Deep Dive**

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

**South Korea**



Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



The guidelines also require organisations to establish strong governance structures for AI privacy compliance, including the mandatory appointment of a Chief Privacy Officer.

**Key elements include:**



Executive accountability



Cross-functional collaboration



Comprehensive documentation for audits



Staff training on privacy practices



Introduction

Overview

Key Data Privacy

Recommendations

**Jurisdictional Deep Dive**

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

**South Korea**



Taiwan (China)

Thailand

Vietnam





Contacts

Endnotes



The governance framework also addresses AI-specific risks such as algorithmic bias, transparency, and the need for human oversight. Furthermore, the guidelines incorporate emerging trends in AI technology and are designed to be updated regularly in response to ongoing advancements and evolving regulatory requirements.

*The PIPC has also published several other guidelines including:*

-  **AI Privacy Risk Management Model for Safe AI Data Utilization** (February 2025) which presents the direction and principles for AI privacy risk management<sup>45</sup>
-  **Synthetic Data Generation and Utilization Guide** (December 2024) which provides reference methods and procedures for generating and utilising synthetic data<sup>46</sup>
-  **Guidelines for Processing Publicly Available Personal Information for AI Development and Services** (July 2024) which includes standards for collecting and using publicly available personal information for AI training and services<sup>47</sup>
-  **AI Personal Information Protection Self-Assessment Checklist** (for Developers and Operators) (July 2021) which provides draft self-assessment items necessary for developing and operating AI systems<sup>48</sup>



Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea



Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



# Taiwan (China)

**The Personal Data Protection Act (PDPA) in Taiwan (China) ("Taiwan") is the primary legislation governing the collection, processing, and use of personal data.<sup>49</sup>**

It originally became effective in October 2012 and the most recent amendments were made in May 2023. The PDPA is accompanied by the Enforcement Rules of the Personal Data Protection Act which were most recently amended in March 2016.<sup>50</sup>

## *Key features of the PDPA include:*



### **Scope**

Applies to both public and private entities handling personal data



### **Data Minimisation**

Encourages the collection of only necessary data for specified purposes



### **Definitions**

Clearly defines personal data and sensitive personal data, establishing categories for protection



### **Consent**

Requires explicit consent from individuals before collecting or processing their personal data



### **Rights of Individuals**

Grants individuals rights to access, correct, and delete their personal data, as well as the right to withdraw consent



### **Data Security**

Mandates measures to protect personal data from breaches, including technical and organisational safeguards



### **Consent Requirements**

Prior consent is needed for collecting sensitive information, for providing personal information for a third party, and for cross-border data transfers (with some exceptions). Individuals must be informed about the purpose of use





### Cross-Border Data Transfers

Regulates the transfer of personal data outside Taiwan, ensuring adequate protection levels in recipient countries



### Penalties

Establishes penalties for non-compliance, including fines and administrative sanctions

The Taiwanese government created an entity to oversee compliance with the PDPA following the amendments made in May 2023. The Preparation Office of Taiwan's Personal Data Protection Commission (PDPC) was established in December 2023. In a similar manner to the PIPA in South Korea, the PDPC does not have explicit rules for data privacy and protection in relation to AI. The PDPC is responsible for creating a data privacy framework within which AI systems are expected to comply and ensure the protection of individuals' data. The MODA has released the *Draft Act on Promoting the Development of Data Innovation and Utilization* ("Draft Act") in August 2025 which advocates data use and sharing as well as creating a legal framework for Taiwan's AI development.<sup>51</sup> The Draft Act will establish data governance regulations for AI use, it demonstrates that Taiwan intends to regulate data concerns relating to AI going forward.



Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)



Thailand

Vietnam

Contacts

Endnotes





# Thailand

The core data privacy regulation in Thailand is the **Personal Data Protection Act (PDPA)** which was passed in 2019 but became effective in June 2022.<sup>52</sup>

In April 2024, Thailand established the *Master Plan for the National Promotion and Protection of Personal Data* ("Master Plan") overseen by the Personal Data Protection Committee (PDPC) and the National Digital Economy and Society Commission.<sup>53</sup> The Master Plan assesses Thailand's personal data protection, outlining current policies, strategies, and objectives from 2024 to 2027.

## Key principles of the PDPA include:



### Cross-Border Transfers

Data transferred outside Thailand must be adequately protected



### Purpose Limitation

Personal data may only be collected for specified, explicit, and legitimate purposes



### Data Subject Rights

Individuals have rights to access, correct, delete, and object to the use of their data



### Data Security

Organisations must implement measures to safeguard personal data against unauthorised or unlawful processing, loss, or damage



### Consent

Data controllers must obtain explicit consent before collecting, using, or disclosing personal data, except for certain legal exemptions (e.g. contractual necessity or legal obligations)



Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand



Vietnam

Contacts

Endnotes



**Key objectives of the Master Plan include:**



Strengthen legal and policy frameworks



Build data protection skills and awareness



Promote public trust in digital services



Support effective governance and compliance

**Key strategies the Master Plan will use to implement its objectives include:**



Update laws and regulations



Train data protection personnel



Run public awareness campaigns



Promote secure technologies



Enhance supervision by the PDPC



Introduction

Overview

Key Data Privacy

Recommendations

**Jurisdictional Deep Dive**

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

**Thailand**



Vietnam

Contacts

Endnotes



The PDPC through the issuance of subordinate laws to the PDPA and the development of the Master Plan are actively developing Thailand's data privacy framework to meet modern demands and business practices. Thailand has not yet established any fixed laws or guidelines relating to data privacy concerns in AI, however the PDPC through the Master Plan demonstrate their intent to develop data privacy regulation in Thailand in line with the changing data environment to prepare for the AI transition.

In June 2025, The Bank of Thailand released draft guidelines for public consultation regarding AI use in financial services, focusing on risk management, transparency, and customer protection.<sup>54</sup> These guidelines apply to financial institutions and payment system operators under Thai law, emphasising accountability, lifecycle risk management, and customer protection. They propose AI usage policies which align with legal standards, risk assessment strategies, human oversight, data and model controls, and cybersecurity measures.



# Vietnam

In Vietnam, the main data privacy regulation is the *Decree on Personal Data Protection* ("the Decree") released in April 2023.<sup>55</sup>

It aims to protect personal data and ensure privacy in the digital economy.

## The Decree:



**Protects personal data** and ensures privacy in the digital economy



Allows cross-border data transfers to countries with adequate data protection laws



**Exempts certain data processing activities**, such as those for national security, defence, and public health



**Ensures data processing is lawful, fair, and transparent**, with specified purposes and minimal data collection



**Grants data subjects the right** to information, access, rectification, erasure, objection, and data portability



**Requires organisations to notify the competent authority and affected data subjects in the event of a data breach**



**Applies to all organisations and individuals processing personal data within Vietnam**, including foreign entities



Enforces the decree through the Ministry of Public Security and other authorities, with **penalties for violations** including administrative fines, suspension of operations, and criminal charges



**Defines personal data** as information that can identify an individual and sensitive personal data as information related to race, ethnicity, political views, religious beliefs, health, and biometric information



Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam



Contacts

Endnotes



On June 26, 2025, the National Assembly of Vietnam promulgated the Law on Personal Data Protection 2025 (“LPDP”), which will take effect on 1 January 2026.<sup>56</sup> The Law sets out regulations on personal data, its protection, as well as the rights, obligations, and responsibilities of relevant agencies, organisations, and individuals.

### Key highlights in LPDP 2025:



#### Prohibition of Data Trading

The law explicitly prohibits the buying and selling of personal data, with significant penalties for violations. This is a major change aimed at curbing illegal data commercialisation



#### Stronger Data Subject Rights

Individuals are granted expanded rights, including the right to be informed about how their data is processed, the right to access and correct their data, and the right to object to or request the erasure of their data. Consent must be explicitly and voluntarily given for specific purposes



#### Severe Penalties

The law introduces strict administrative and criminal penalties for non-compliance. Fines can be up to 5% of a company's total annual revenue in Vietnam for serious violations. Penalties for illegal data trading can be up to 10 times the illicit profits



#### Strict Obligations for Organisations

Data controllers and processors are now required to implement robust security measures to protect personal data. Key obligations include providing clear data processing notifications to individuals and reporting data breaches to both the competent authorities and the affected data subjects. A notable new requirement is the mandatory deletion of a job applicant's data if they are not hired





# Contacts

## Authors



**Nicola Sergeant**  
**Managing Director**  
ACRS Operations Lead  
Japan  
[nicola.sergeant@tohatsu.co.jp](mailto:nicola.sergeant@tohatsu.co.jp)



**Rhys Belcher**  
**Senior Consultant**  
ACRS  
Hong Kong SAR  
[jobelcher@deloitte.com.hk](mailto:jobelcher@deloitte.com.hk)

## Asia Pacific Centre for Regulatory Strategy (ACRS)



**Seiji Kamiya**  
**Executive Sponsor**  
Asia Pacific Regulatory & Financial Risk Lead  
[seiji.kamiya@tohatsu.co.jp](mailto:seiji.kamiya@tohatsu.co.jp)



**Yuki Shuto**  
**ACRS Steering Committee**  
Partner  
AP Consulting Growth Leader  
[yshuto@tohatsu.co.jp](mailto:yshuto@tohatsu.co.jp)



**Tony Wood**  
**ACRS Steering Committee**  
Partner  
AP Banking & Capital Markets Leader  
[tonywood@deloitte.com.hk](mailto:tonywood@deloitte.com.hk)



**Ye Fang**  
**ACRS Steering Committee**  
Partner  
China SR&T FS Industry Lead  
[yefang@deloitte.com.cn](mailto:yefang@deloitte.com.cn)



**Sean Moore**  
**Australia Co-lead**  
Partner  
AU SR&T FS Industry Lead  
[semoore@deloitte.com.au](mailto:semoore@deloitte.com.au)



**Nai Seng Wong**  
**SEA Co-lead**  
Partner  
SEA Regulatory Strategy Lead  
[nawong@deloitte.com](mailto:nawong@deloitte.com)



**Shinya Kobayashi**  
**Japan Co-lead**  
Managing Director  
JP SR&T Insurance Sector Lead  
[shinya.kobayashi@tohatsu.co.jp](mailto:shinya.kobayashi@tohatsu.co.jp)

Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



## Asia Pacific Trustworthy AI Leaders



**Dr Elea Wurth**  
**Partner**  
Asia Pacific & Australia  
[ewurth@deloitte.com.au](mailto:ewurth@deloitte.com.au)



**Amy Dove**  
**Partner**  
New Zealand  
[amydove@deloitte.co.nz](mailto:amydove@deloitte.co.nz)



**Toyohiro Sometani**  
**Partner**  
Japan  
[toyohiro.sometani@tohatsu.co.jp](mailto:toyohiro.sometani@tohatsu.co.jp)



**Chris A. Chen**  
**Partner**  
Taiwan  
[chrisachen@deloitte.com.tw](mailto:chrisachen@deloitte.com.tw)



**Jessica Kim**  
**Partner**  
South Korea  
[jessikim@deloitte.com](mailto:jessikim@deloitte.com)



**Silas Hao Zhu**  
**Partner**  
China  
[silzhu@deloitte.com.cn](mailto:silzhu@deloitte.com.cn)



**Dishell Gokaldas**  
**Partner**  
Singapore  
[dgokaldas@deloitte.com](mailto:dgokaldas@deloitte.com)



**Jayant Saran**  
**Partner**  
India  
[jsaran@deloitte.com](mailto:jsaran@deloitte.com)



**Pence Cong Peng**  
**Partner**  
China  
[pepeng@deloitte.com.cn](mailto:pepeng@deloitte.com.cn)



**Brad Puye Lin**  
**Partner**  
Hong Kong SAR  
[bradlin@deloitte.com.hk](mailto:bradlin@deloitte.com.hk)

Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



## Contributors



**Harm Ellens**  
**AI Governance &  
Risk Management Specialist**  
Director  
Australia  
[hellens@deloitte.com.au](mailto:hellens@deloitte.com.au)



**Mayuran Palanisamy**  
**Digital Privacy &  
Trust Offering Leader**  
Partner  
India  
[mayuranp@deloitte.com](mailto:mayuranp@deloitte.com)



**Lucy Mannering**  
**Privacy  
Leader**  
Partner  
Australia  
[lmannering@deloitte.com.au](mailto:lmannering@deloitte.com.au)



**Han H. Lin**  
**Privacy &  
Data Protection Specialist**  
Managing Director  
Taiwan  
[hanhlin@deloitte.com.tw](mailto:hanhlin@deloitte.com.tw)



**Toshiyuki Oba**  
**Privacy, Security &  
IT Governance Specialist**  
Managing Director  
Japan  
[toshiyuki.oba@tohatsu.co.jp](mailto:toshiyuki.oba@tohatsu.co.jp)



**Mariette Van Niekerk**  
**Data Science  
Lead**  
Managing Director  
New Zealand  
[mvanniekerk@deloitte.co.nz](mailto:mvanniekerk@deloitte.co.nz)

Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts

Endnotes



## Acknowledgements

**Tommy Hartanto**  
**Director**

Indonesia  
[thartanto@deloitte.com](mailto:thartanto@deloitte.com)

**Joey Xu**  
**Senior Manager**

China  
[joexu@deloittecn.com.cn](mailto:joexu@deloittecn.com.cn)

**Herbert Rollom**  
**Director**

Philippines  
[hrollom@deloitte.com](mailto:hrollom@deloitte.com)

**Andy T. Tsou**  
**Manager**

Taiwan  
[atsou@deloitte.com.tw](mailto:atsou@deloitte.com.tw)

**Dae Woo Lee**  
**Manager**

Korea  
[dlee37@deloitte.com](mailto:dlee37@deloitte.com)

**Anh Quoc Luu**  
**Senior Manager**

Vietnam  
[anhqluu@deloitte.com](mailto:anhqluu@deloitte.com)

**Kerrie Hie**  
**Director**

Australia  
[khie@deloitte.com.au](mailto:khie@deloitte.com.au)

**Shoya Kusoda**  
**Senior Consultant**

Japan  
[shoya.kusuda@tohatsu.co.jp](mailto:shoya.kusuda@tohatsu.co.jp)

**Eric Kanikevich**  
**Consultant**

Australia  
[ekanikevich@deloitte.com.au](mailto:ekanikevich@deloitte.com.au)

**Fransisca Fransisca**  
**Manager**

Hong Kong  
[fransisca@deloitte.com.hk](mailto:fransisca@deloitte.com.hk)

**Jane Zhang**  
**Associate Director**

China  
[janezhang@deloittecn.com.cn](mailto:janezhang@deloittecn.com.cn)

**Christina Fialova**  
**Consultant**

Singapore  
[cfialova@deloitte.com](mailto:cfialova@deloitte.com)

**Steven S. Fang**  
**Manager**

Taiwan  
[stefang@deloitte.com.tw](mailto:stefang@deloitte.com.tw)

**Prakash Arikrishnan**  
**Director**

Malaysia  
[parikrishnan@deloitte.com](mailto:parikrishnan@deloitte.com)

**Monai Supanit**  
**Senior Manager**

Thailand  
[msupanit@deloitte.com](mailto:msupanit@deloitte.com)

**Tony Zhi-Wei Tang**  
**Associate Director**

Australia  
[totang@deloitte.com.au](mailto:totang@deloitte.com.au)

**Samuel Yue Xuan Ang**  
**Consultant**

Singapore  
[saang@deloitte.com](mailto:saang@deloitte.com)

Introduction

Overview

Key Data Privacy

Recommendations

Jurisdictional Deep Dive

Australia

China (Mainland)

Hong Kong SAR

India

Indonesia

Japan

Malaysia

New Zealand

Philippines

Singapore

South Korea

Taiwan (China)

Thailand

Vietnam

Contacts



Endnotes



# Endnotes

1. Deloitte Center for Government Insights, *The AI regulations that aren't being talked about*, November 2023, [AI regulation | Deloitte Insights](#)
2. Deloitte Asia Pacific AI Institute, *AI at a crossroads – Building trust as the path to scale*, January 2025, [AI at a crossroads | Deloitte China](#)
3. Deloitte Centre for Technology, Media and Telecommunications, *Data privacy and security worries are on the rise, while trust is down*, September 2023, [Consumer data privacy and security | Deloitte Insights](#)
4. Deloitte US, *Third Edition: State of Ethics and Trust in Technology*, September 2024, [Deloitte's 2024 ethical technology report | Deloitte US](#)
5. Capgemini Research Institute, *"AI and the ethical conundrum" Report*, October 2020, [AI and the ethical conundrum: How organisations can build ethically robust AI systems and gain trust - Capgemini](#)
6. Lonergan Research, *DPSI Consumer Survey Research Report*, February 2025, [dpsi-consumer-survey-research-report-lonergan-research-feb2025.pdf](#)
7. European Parliament, *General Data Protection Regulation (GDPR)*, April 2016, [Regulation - 2016/679 - EN - gdpr - EUR-Lex](#)
8. European Parliament, *General Data Protection Regulation (GDPR)*, April 2016, [Regulation - 2016/679 - EN - gdpr - EUR-Lex](#)
9. Office of the Australian Privacy Commissioner, *OAIC stats show record year for data breaches*, May 2025, [OAIC stats show record year for data breaches | OAIC](#)
10. Australian Government, *Privacy and Other Legislation Amendment Bill 2024*, December 2024, [Privacy and Other Legislation Amendment Bill 2024 – Parliament of Australia](#)
11. Australian Government, *Privacy Act 1988*, December 1988, [Privacy Act 1988 - Federal Register of Legislation](#)
12. Australian Government, *Australian Privacy Principles*, [Australian Privacy Principles | OAIC](#)
13. Office of the Australian Privacy Commissioner, *Guidance on privacy and the use of commercially available AI products*, October 2024, [Guidance on privacy and the use of commercially available AI products | OAIC](#)
14. Office of the Australian Privacy Commissioner, *Guidance on privacy and developing and training generative AI models*, October 2024, [Guidance on privacy and developing and training generative AI models | OAIC](#)
15. Office of the Australian Privacy Commissioner, *Joint statement on building trustworthy data governance frameworks to encourage development of innovative and privacy-protective AI*, February 2025, [Joint statement on building trustworthy data governance frameworks to encourage development of innovative and privacy-protective AI | OAIC](#)
16. National People's Congress, *Personal Information Protection Law*, November 2021, [http://en.npc.gov.cn.cdurl.cn/2021-12/29/c\\_694559.htm](#)
17. National People's Congress, *Data Security Law of the People's Republic of China*, June 2021, [Data Security Law of the People's Republic of China](#)
18. National Financial Regulatory Administration, *Rules on Data Security of Banking and Insurance Institutions*, December 2024, [NFRA](#)
19. Cyberspace Administration of China, *Interim Measures for the Management of Generative Artificial Intelligence Services*, July 2023, [http://www.cac.gov.cn/2023-07/13/c\\_1690898327029107.htm](#)
20. Office of the Privacy Commissioner for Personal Data Hong Kong, *Personal Data (Privacy) Ordinance*, August 1995, [《個人資料\(私隱\)條例》 Personal Data \(Privacy\) Ordinance](#)
21. Office of the Privacy Commissioner for Personal Data Hong Kong, *Personal Data (Privacy) (Amendment) Ordinance 2021*, October 2021, [s12021254032](#)
22. Office of the Privacy Commissioner for Personal Data Hong Kong, *Artificial Intelligence: Model Personal Data Protection Framework*, June 2024, [ai\\_protection\\_framework.pdf](#)
23. Office of the Privacy Commissioner for Personal Data Hong Kong, *Guidance on the Ethical Development and Use of Artificial Intelligence*, August 2021, [pcpd.org.hk/english/resources\\_centre/publications/files/guidance\\_ethical\\_e.pdf](#)
24. Parliament of India, *The Digital Personal Data Protection Act, 2023*, August 2023, [2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf](#)
25. Government of India, *Digital Personal Data Protection Rules, 2025*, January 2025, [Draft Digital Personal Data Protection Rules, 2025 – Innovate India](#)
26. Government of Indonesia, *Law of the Republic of Indonesia Number 27 of 2022 Concerning Personal Data Protection*, October 2022, [Salinan UU Nomor 27 Tahun 2022.pdf](#)
27. Japanese Government, *Act on the Protection of Personal Information*, May 2003, [Act on the Protection of Personal Information - English - Japanese Law Translation](#)
28. Personal Information Protection Commission, *Interim Report on Considerations for the Triennial Review of the Act on Protection of Personal Information*, June 2024, [個人情報保護法 いわゆる3年ごとに見直しに係る検討の中間整理-個人情報保護委員会-](#)
29. Personal Information Protection Commission, *Precautionary Notice on Use of Generative AI Services*, June 2023, [生成AIサービスの利用に関する注意喚起等について（令和5年6月2日） | 個人情報保護委員会](#)
30. Parliament of Malaysia, *Personal Data Protection Act 2010 (Act 709)*, June 2010, [PDP Act 2010 • Protection of Personal Data](#)





# Endnotes

31. Parliament of Malaysia, *Personal Data Protection (Amendment) Act 2024*, October 2024, [PDP \(Amendment\) Act 2024 • Protection of Personal Data](#)

32. New Zealand Government, *Privacy Act 2020*, June 2020, [Privacy Act 2020 No 31 \(as at 30 March 2025\), Public Act Contents – New Zealand Legislation](#)

33. New Zealand Privacy Commissioner, *Artificial Intelligence and the Information Privacy Principles*, September 2023, [AI-and-the-Information-Privacy-Principles.pdf](#)

34. National Privacy Commission, *Data Privacy Act, 2012*, August 2012, [Republic Act 10173 - Data Privacy Act of 2012 - National Privacy CommissionNational Privacy Commission](#)

35. National Privacy Commission, *Joint Advisory - Considerations on the Use Of Privacy Enhancing Technologies (PETs) In The Insurance Industry*, March 2025, [NPC-IC-Joint-Advisory-2025.03.11-Considerations-on-the-Use-of-PETs-in-the-Insurance-Industry-w-SGD.pdf](#)

36. National Privacy Commission, *Guidelines on The Application of Republic Act No. 10173 or the Data Privacy Act Of 2012 (DPA), Its Implementing Rules and Regulations, and the Issuances of the Commission to Artificial Intelligence Systems Processing Personal Data*, December 2024, [Advisory-2024.12.19-Guidelines-on-Artificial-Intelligence-w-SGD.pdf](#)

37. Singapore Government, *Personal Data Protection Act 2012*, October 2012, [Personal Data Protection Act 2012 - Singapore Statutes Online](#)

38. Singapore Government, *Personal Data Protection (Amendment) Act 2020*, December 2020, [Personal Data Protection \(Amendment\) Act 2020 - Singapore Statutes Online](#)

39. Personal Data Protection Commission, *Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems*, March 2024, [advisory-guidelines-on-the-use-of-personal-data-in-ai-recommendation-and-decision-systems.pdf](#)

40. Infocomm Media Development Authority (IMDA), [Privacy Enhancing Technology Sandbox, Privacy Enhancing Technology Sandboxes | IMDA](#)

41. Personal Data Protection Commission (PDPC), *Proposed Guide to Synthetic Data Generation*, July 2024, [proposed-guide-on-synthetic-data-generation.pdf](#)

42. Personal Information Protection Commission, Korea, *Personal Information Protection Act*, September 2023, [PIPC, Korea, GPA, 2025 GPA, GPA Seoul, 2025 GPA Seoul, AI, Data, Privacy, GPA 서울, Global Privacy Assembly](#)

43. Personal Information Protection Commission, Korea, *Amended Personal Information Protection Act (PIPA) and its Enforcement Decree Become Effective*, September 2023, [PIPC, Korea, GPA, 2025 GPA, GPA Seoul, 2025 GPA Seoul, AI, Data, Privacy, GPA 서울, Global Privacy Assembly](#)

44. Personal Information Protection Commission, Korea, *The PIPC Sets Out Personal Data Processing Criteria for Generative AI*, August 2025, [PIPC, Korea, GPA, 2025 GPA, GPA Seoul, 2025 GPA Seoul, AI, Data, Privacy, GPA 서울, Global Privacy Assembly](#)

45. Personal Information Protection Commission, Korea, *AI Privacy Risk Management Model for Safe Utilization of AI and Data*, December 2024, [Press Release Details | Personal Information Protection Commission](#)

46. Personal Information Protection Commission, Korea, *PIPC Unveils Guidelines on Generating and Utilizing Synthetic Data*, December 2024, [PIPC, Korea, GPA, 2025 GPA, GPA Seoul, 2025 GPA Seoul, AI, Data, Privacy, GPA 서울, Global Privacy Assembly](#)

47. Personal Information Protection Commission, Korea, *Guideline on Processing Publicly Available Data for AI Development and Services*, July 2024, [PIPC, Korea, GPA, 2025 GPA, GPA Seoul, 2025 GPA Seoul, AI, Data, Privacy, GPA 서울, Global Privacy Assembly](#)

48. Personal Information Protection Commission, Korea, *AI Personal Information Protection Self-checklist*, July 2021, [PIPC, Korea, GPA, 2025 GPA, GPA Seoul, 2025 GPA Seoul, AI, Data, Privacy, GPA 서울, Global Privacy Assembly](#)

49. Government of the Republic of China (Taiwan), *Personal Data Protection Act*, May 2023, [Personal Data Protection Act - Article Content - Laws & Regulations Database of The Republic of China \(Taiwan\)](#)

50. Government of the Republic of China (Taiwan), *Enforcement Rules of the Personal Data Protection Act*, March 2016, [Enforcement Rules of the Personal Data Protection Act - Article Content - Laws & Regulations Database of The Republic of China \(Taiwan\)](#)

51. Ministry of Digital Affairs, *Draft Act on Promoting the Development of Data Innovation and Utilization Released for Public Consultation*, August 2025, [Draft Act on Promoting the Development of Data Innovation and Utilization Released for Public Consultation — the Ministry of Digital Affairs Drives Data Sharing and AI Development | Press Releases - News and Releases | Ministry of Digital Affairs](#)

52. Personal Data Protection Committee, *Personal Data Protection Act*, May 2019, [Personal Data Protection Act B.E. 2562 \(2019\) - PDPC](#)

53. Personal Data Protection Committee, *Master Plan for the National Promotion and Protection of Personal Data*, April 2024, [แผนแม่บทการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลของประเทศ พ.ศ. 2567 - 2570 - PDPC](#)

54. Bank of Thailand, *Hearing on the Draft Bank of Thailand Policy Guidelines Risk Management of Artificial Intelligence System*, June 2025, [\(Draft\) Bank of Thailand Policy Guidelines Risk Management of Artificial Intelligence System](#)

55. Government of Vietnam, *Decree 13/2023/ND-CP on Personal Data Protection*, April 2023, [13/2023/ND-CP in Vietnam, Decree No. 13/2023/ND-CP dated April 17, 2023 on protection of personal data in Vietnam](#)

56. National Assembly of Vietnam, *Law of Personal Data Protection 2025*, June 2025, [https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Luat-Bao-ve-du-lieu-ca-nhan-2025-so-91-2025-QH15-625628.aspx?dll=true](#)





The Deloitte Centre for Regulatory Strategy is a source of critical insights and advice, designed to assist the world's largest financial institutions manage the strategic and aggregate impact of regional and international regulatory policy. With regional hubs in Asia Pacific, the Americas and EMEA, the Centre combines the strength of Deloitte's network of experienced risk, regulatory, and industry professionals — including a deep roster of former regulators, industry specialists, and business advisers — with a rich understanding of the impact of regulations on business models and strategy.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organisation"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](https://www.deloitte.com/about) to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organisation") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 415,000 people make an impact that matters at [www.deloitte.com](https://www.deloitte.com).

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, or the Deloitte organisation is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte organisation.