ISSUE BRIEF

GLOBAL

# Regulatory Strategies of Data Protection Authorities in the Asia-Pacific Region: 2024, and Beyond

Authors: Dominic Paulger, Bilal Mohamed, Sakshi Shivhare, Brendan Tan
Editors: Josh Lee Kok Thong and Lee Matheson
September 2024

FUTURE OF PRIVACY FORUM

# Table of Contents

# Introduction

The Asia-Pacific (APAC) region has emerged as a dynamic and rapidly evolving landscape for data protection regulation. As digital economies flourish and cross-border data flows intensify, data protection authorities (DPAs) across the region are grappling with complex challenges posed by technological advancements, changing business practices, and evolving societal expectations regarding privacy.

This Report provides a comprehensive analysis of strategy documents and key regulatory actions of the DPAs in 10 jurisdictions, published or developed in 2023 and 2024, setting out regulatory priorities for the following years:

1. **Australia**
2. **China**
3. **Hong Kong, Special Administrative Region of China (SAR)**
4. **Japan**
5. **Malaysia**
6. **New Zealand**
7. **Philippines**
8. **Singapore**
9. **South Korea**
10. **Thailand**

The Report is structured into two sections.

- The first provides an overview of key trends in the APAC region and identifies priority areas and future initiatives that APAC DPAs indicate that they will focus on in years to come.
- The second provides a brief profile of each DPA and summarizes their regulatory actions for the period of 2023-2024, as well as any key strategy documents available.

Our analysis provides insights into how these DPAs have been working towards implementing their strategic priorities throughout 2023 and 2024. To the extent possible, the analysis in this Report is based on official strategy documents – that is, master plans, statements of regulatory priorities, annual reports, and the like – published by these DPAs between 2023-2024, supplemented by an examination of significant regulators actions taken by the DPAs during this period.

While we offer a thorough examination of recent and ongoing initiatives, it is important to note that the data protection landscape is dynamic and rapidly evolving. Therefore, this report not only serves as a *retrospective* overview but also aims to highlight *prospective* directions that DPAs may pursue in 2025 and beyond. By highlighting the trajectory of these regulatory bodies, we hope that this Report will aid readers in anticipating

potential developments in data protection regulation and enforcement across the region. However, readers should bear in mind that unforeseen technological advancements, geopolitical shifts, or other factors may influence future regulatory approaches in ways that cannot be fully predicted at the time of publication.

The Report recognizes that each jurisdiction faces unique challenges, operates within distinct legal and cultural contexts, and may prioritize different aspects of data protection based on their specific circumstances. The Report is therefore not intended to make value judgments on DPAs, rank them, or evaluate their effectiveness in key areas. Rather, our aim is to identify commonalities and divergences in the DPAs' priorities and approaches, in order to shed light on key trends in the APAC region. We hope that these insights will prove useful to policymakers, businesses, and data protection privacy professionals as they navigate the APAC region's complex data protection landscape.

To ensure a comprehensive and accurate understanding of this Report's scope and methodology, readers should note the following key considerations:

- Not all the above DPAs consistently publish official strategy documents. Where a given DPA has not published a strategy document for the period of 2023-2024, the Report's analysis infers the relevant DPA's priorities from its regulatory actions.
- Not all the above DPAs provide official documents and information in English. Where official English language translations of relevant documents and information are unavailable, we have worked from machine translations.
- Our analysis focuses primarily on the DPAs' strategies and priorities regarding the private sector. While public sector data protection is an important area, it often raises distinct considerations which are beyond the aims of this Report.

Analysis of key strategic documents and recent regulatory actions across the 10 APAC DPAs reveals several common priorities for 2024 and beyond.

- **Cybersecurity and data breach response** emerged as the most widespread priority, with 90% of the DPAs prioritizing efforts to combat cyber threats and enhance organizational readiness for data breaches. This reflects the growing frequency and sophistication of cyber attacks across the region and globally.
- **Cross-border data transfers** were a key priority for 80% of the DPAs, highlighting the increasing importance of facilitating secure international data flows in an interconnected digital economy.
- **AI governance and regulation** was a key focus for 70% of the DPAs, as authorities grappled with the rapid advancement and adoption of AI technologies, particularly generative AI, in recent years.
- **Regulation of the use of biometric data**, including facial recognition technology (FRT), was prioritized by 60% of DPAs, indicating growing concerns about the privacy implications of these technologies.
- Finally, 50% of DPAs emphasized the **protection of children's personal data**, recognizing the unique needs of young people in digital environments

# Part 1: Regional Trends

## The Data Protection Landscape in APAC

As of September 2024, the majority of major jurisdictions in APAC now have comprehensive national data protection laws. However, the data protection landscape in APAC is marked by significant diversity, reflecting the region's varied legal traditions, economic development levels, and approaches to data governance.

This landscape has evolved over three decades and continues to develop. Some jurisdictions are working to modernize their data protection frameworks to align with international practices and respond to evolving technological and societal challenges, while others are focusing on implementing and interpreting recently updated or newly enacted laws.

The **first generation** of data protection laws in APAC date back to the late 1980s and early 1990s. This first generation of APAC data protection laws includes:

- **Australia's** Privacy Act (1988, substantially amended in 2014, 2018, and 2022);
- **New Zealand**'s Privacy Act (originally enacted in 1993 but updated and reissued in 2020); and
- **Hong Kong SAR's** Personal Data (Privacy) Ordinance (1996, substantially amended in 2012 and 2021).

Notably, all these laws were based on the **OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**, which were adopted in 1980,[1] and so share many common features, including giving effect to a set of technology-neutral privacy principles. While retaining these core features, all of these laws have since been substantially amended – further detail on these amendments is provided in Part 2 of this Report.

This **second generation** of APAC data protection laws emerged between the 2000s and early 2010s. These include:

- **Japan's** Act on the Protection of Personal Information (2003, substantially amended in 2015, 2020, and 2021);
- **Macau SAR**'s Personal Data Protection Act (2005);
- **Taiwan**'s Personal Data Protection Act (2010);
- **South Korea**'s Personal Information Protection Act (2011, substantially amended in 2020 and 2023); and
- **Singapore**'s Personal Data Protection Act (2012, substantially amended in 2021).

This generation is characterized by a diversity of different approaches to data protection. However, the influence of European data protection law began to emerge in the laws of Macau, which drew directly from the European

[1] https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en

Union (EU)'s Directive 95/46, and South Korea, which adopted several similar provisions to those in the Directive. Several of these laws have since been substantially amended - further detail on these amendments is provided in Part 2 of this Report.

The **third generation** of APAC data protection laws emerged following the enactment of the EU's General Data Protection Regulation (GDPR) in 2016. These laws include:

- **Laos**' Law on Electronic Data Protection (2017);
- **Thailand**'s Personal Data Protection Act (2019);
- **China's** Personal Information Protection Law (2021);
- **Mongolia**'s Data Protection Law (2021),
- **Sri Lanka's** Personal Data Protection Act (2022);
- **Indonesia**'s Personal Data Protection Law (2022);
- **Vietnam**'s Personal Data Protection Decree (2023), and
- **India**'s Digital Personal Data Protection Act (2023).

Many of these laws drew inspiration from the GDPR to varying degrees. However, not all these laws are currently operational. In particular, as of the date of this Report, the data protection laws of India and Indonesia have yet to take effect, and several key provisions still need to be fully implemented through subordinate regulations.

The data protection landscape in APAC is far from static. Notably, several first and second-generation APAC data protection laws are subject to review in 2024.

- **Australia**'s government has been conducting a comprehensive review of the Privacy Act and tabled a bill to amend the Act in September 2024.
- **Hong Kong**'s government has been working on potential amendments to the Personal Data (Privacy) Ordinance since February 2023.
- **Japan**'s Act on the Protection of Personal Information is currently undergoing a mandatory three-year review, but no immediate amendments are planned.
- In July 2024, a bill to amend **Malaysia**'s Personal Data Protection Act was passed by both houses of Malaysia's Parliament. As of the publication of this report, the bill is awaiting Royal Assent.
- Minor amendments to **New Zealand**'s Privacy Act are already underway, and there have been calls (especially from New Zealand's DPA) to further update its framework.

# Data Protection Authorities in the APAC Region

A critical aspect in operationalizing effective data protection frameworks in APAC is the establishment of dedicated regulatory authorities. As of August 2024, only 10 jurisdictions in the region have **operational** DPAs, namely:

| Jurisdiction | Authority |
|---|---|
| **Australia** | The **Office of the Australian Information Commissioner** (OAIC), established in 2010. |
| **China** | The **Cyberspace Authority of China** (CAC), established as a cyberspace regulator in 2014 and assigned administrative responsibility for personal data protection in 2021. |
| **Hong Kong SAR** | The **Office of the Privacy Commissioner for Personal Data** (OPCPD), established in 1996. |
| **Japan** | The **Personal Information Protection Commission** (PPC), established in 2016. |
| **Malaysia** | The **Personal Data Protection Department** (PDPD), established in 2011. |
| **New Zealand** | The **Office of the Privacy Commissioner** (OPC), established in 1993. |
| **Philippines** | The **National Privacy Commission** (NPC), established in 2016. |
| **Singapore** | The **Personal Data Protection Commission** (PDPC), established in 2013.[2] |
| **South Korea** | The **Personal Information Protection Commission** (PIPC), established in 2011. |
| **Thailand** | The **Personal Data Protection Commission** (PDPC), established in 2022. |

[2] Note that since 2016, administrative responsibility passed to the Infocomm Media Development Authority (IMDA), but the Personal Data Protection Commission name and branding was retained.

It is worth noting that **Macau SAR** recently replaced its DPA. In 2007, Macau established the Office for Personal Data Protection (OPDP) as a temporary regulatory and enforcement body. In 2023, as part of efforts to streamline public services and reorganize temporary project units in Macau, the OPDP was restructured into the Personal Data Protection Bureau (PDPB) via Administrative Regulation No. 42/2023.[3] The PDPB is a permanent bureau within Macau's Public Administration and is under the direct authority of the Chief Executive. As the new PDPB is still in the process of becoming operational and has not released information on its strategic priorities going forward, we have omitted it from the scope of this Report.

There is considerable variation in how active each of these DPAs is, reflecting differences in the age of their data protection laws, regulatory approaches, and national priorities. For instance:

- DPAs in **Australia**, **Hong Kong SAR**, **New Zealand, Singapore**, and **South Korea** have been in operation for a considerable time and demonstrate moderate to high levels of activity. They regularly publish comprehensive guidance, engage in enforcement actions, and participate actively in international fora. Their consistency in regulatory activity has allowed them to develop more distinct and sophisticated regulatory approaches, as well as to take more proactive stances to address issues brought about by emerging technologies.
- DPAs in **China**, **Japan**, and **the Philippines** – despite having been established more recently – have quickly established themselves as highly active regulators. They have also engaged in significant rulemaking and shown increasing enforcement activity. Their rapid development may be attributed to strong governmental support and the pressing need to regulate fast-evolving digital economies.
- **Malaysia**'s PDPD has been comparatively less active in recent years, while **Thailand**'s PDPC (which was established in 2022) has been building up its organizational capacity and has only recently shifted from rulemaking to enforcement.

[3] https://www.dspdp.gov.mo/en/company_profile.html

# APAC Data Protection Authorities' Strategy Documents

APAC DPAs differ in whether they publish strategy documents, how regularly they do so, and what the scope of these documents is.

DPAs in certain jurisdictions (such as Australia, Japan, New Zealand, and South Korea) consistently publish strategy documents while others (such as Malaysia) do so sporadically, and still others (such as China and Singapore) do not release such documents at all. Broadly, the 10 DPAs may be categorized into 3 groups:

| Regularity of publishing | Jurisdiction |
|---|---|
| **Regular** | **Australia**'s OAIC publishes an annual Corporate Plan and regularly updates its Regulatory Action Policy. |
| | **Japan**'s PPC publishes annual Activity Policies, International Strategies, and Monitoring and Supervision Policies, which together form a comprehensive view of its strategic priorities. |
| | **New Zealand**'s OPC releases annual Statements of Intent and Statements of Performance Expectations, providing clear, forward-looking strategic information. |
| | **South Korea**'s PIPC releases a triennial Basic Plan for Personal Data Protection and annual Work Plans, offering a clear strategic outlook. |
| **Intermittent or Partial** | **Hong Kong**'s PCPD provides some strategic information through its annual reports and Legislative Council briefings, but these are less comprehensive than those in the first group. |
| | **Thailand**'s PDPC, being newly established, has only recently published its first strategic plan (Master Plan for 2024-2027), and it remains to be seen if this will become a regular practice. |
| | **Philippines**' NPC publishes an annual report. The latest available report covered 2022 and was released in August 2023. |

| | |
|---|---|
| **Limited or None** | **China**'s CAC and **Singapore**'s PDPC do not publish a comprehensive standalone strategy document. While their priorities can be inferred from its regulatory actions and published updates, these may lack the cohesive strategic overview found in more comprehensive documents |
| | **Malaysia**'s PDPD regularly published annual reports between 2014 and 2021. However, it has not published an annual report since 2021. |

For jurisdictions that publish some kind of strategy document, there are contrasts as to the type of documents that they release and whether it is **forward-looking** (outlining long-term visions and planned initiatives of the data protection authorities) or **retrospective** (describing key milestones and achievements in the past year).

## Forward-Looking Strategy Documents

The majority of the 10 jurisdictions publish a forward-looking strategy document. However, among those who publish, they differ on the time horizons of their strategies. Further, among jurisdictions whose DPAs publish forward-looking strategy documents, a further distinction can be drawn between **single-year approaches** (which present objectives for the immediate year ahead) and **multi-year approaches** (which present both long-term, multi-year strategic objectives and shorter term, immediate year objectives).

| Approach | Jurisdiction |
|---|---|
| **Forward-Looking, Multi-Year Approaches** | **Australia**'s OAIC publishes a Corporate Plan that covers a four-year period, outlining long-term strategic priorities and performance measures. This allows stakeholders to understand not just immediate priorities, but also how the OAIC envisions its role evolving over time. |
| | **South Korea**'s PIPC has published a Basic Plan for Personal Data Protection providing a long-term strategic outlook over a three-year period. This is supplemented by annual Work Plans that provide more detailed, short-term objectives within the context of the broader strategy. This approach allows for a balance between long-term vision and flexibility to address emerging issues. |
| | **New Zealand**'s OPC releases a Statement of Intent that spans a four-year period, complemented by annual Statements of Performance Expectations. This combination provides both a long-term strategic view and more immediate operational goals. |
| | **Thailand**'s PDPC appears to be taking this approach through its forward-looking, four-year Master Plan, which covers the period of 2024 to 2027. However, it |

| | |
|---|---|
| | remains to be seen whether PDPC TH will continue to adopt this approach in the future. |
| **Forward Looking, Single-Year Approaches** | **Japan**'s PPC, while not publishing a single comprehensive multi-year strategy document, does provide forward-looking insights through its annual Activity Policy and International Strategy. These documents, while focused on the upcoming year, often include references to longer-term goals and initiatives, particularly in areas like international data transfers and emerging technologies. |

## Retrospective Strategy Documents

By contrast, some jurisdictions do not regularly publish a forward-looking strategy and instead, publish only a **retrospective** strategy document, such as annual reports, that typically place a much greater focus on detailing past activities rather than identifying future priorities and strategies. These jurisdictions include:

- **Malaysia**: As noted above, Malaysia's PDPD regularly published annual reports between 2014 and 2021. However, based on publicly available information on its website, it has not published an annual report since 2021.
- **The Philippines**: The NPC publishes annual reports. The latest available report covered 2022 and was released in August 2023.

It is important to note that jurisdictions in this category primarily rely on annual reports to indicate regulatory priorities, but they may also issue from time to time other types of communications such as press releases, circulars, or advisories. These tend to be more focused on immediate priorities or recent activities. While these documents may mention long-term goals, such goals are often not elaborated upon in the same detail as seen in jurisdictions that regularly publish separate, comprehensive strategy documents.

This variation in the publication of concrete strategy documents reflects differences in regulatory approaches, transparency levels, and possibly the maturity of data protection regimes across these jurisdictions. The variation also impacts the ability of organizations and the public to understand and anticipate regulatory priorities and actions in each jurisdiction.

# Regulatory Priorities

Analysis of key strategic documents and recent regulatory actions across the 10 APAC DPAs reveals that they have been pursuing diverse objectives from 2023 to 2024. Although no single priority is shared by all the DPAs, it is possible to identify several regional trends.

## Regional Priorities Across APAC DPAs At a Glance

1 Cybersecurity and Data Breaches

2 Promoting Cross-Border Data Transfers

3 Artificial Intelligence (AI)

4 Biometrics and FRT

5 Protecting Children's Personal Data

## Overview

The table below provides an overview of priorities reflected in the strategic documents and recent regulatory actions of the 10 APAC DPAs, organized into 8 categories:

1. cybersecurity and data breaches;
2. cross-border data transfers;
3. emerging technologies (including subcategories for AI, automated decision-making, and biometrics and facial recognition technologies);
4. protecting children's personal data;
5. developing the data protection ecosystem (with subcategories for certifications and trustmarks, registration of organizations or processing activities, and DPO requirements);
6. privacy techniques (with subcategories for privacy enhancing technologies (PETs), anonymization, and pseudonymization;
7. data portability; and
8. doxxing.

We note that the absence of a checkmark does not necessarily mean the jurisdiction is not addressing that priority at all, but rather that it was not prominently mentioned in key strategic documents. Overall, the table indicates a **robust and diverse approach to data protection across the region**, with jurisdictions balancing common challenges with nation-specific priorities.

| Priority | AU | CN | HK | JP | MY | NZ | PH | SG | KO | TH |
|---|---|---|---|---|---|---|---|---|---|---|
| **Cybersecurity and Data Breaches** | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Cross-Border Data Transfers** | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |
| **Emerging Technologies** | | | | | | | | | | |
| *AI* | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | |
| *Automated Decision Making* | | ✓ | | ✓ | | | | | ✓ | |
| *Biometrics and FRT* | ✓ | ✓ | ✓ | ✓ | | ✓ | | | ✓ | |
| **Protecting Children's Data** | | ✓ | | ✓ | | ✓ | | ✓ | ✓ | |
| **Developing the Data Protection Ecosystem** | | | | | | | | | | |
| *Certifications and Trustmarks* | | | | ✓ | | | ✓ | ✓ | ✓ | |
| *Registration* | | | | | ✓ | | ✓ | | | |
| *DPO* | | | | | | | ✓ | | ✓ | |
| **Privacy Techniques** | | | | | | | | | | |
| *PETs* | | | | ✓ | | | | ✓ | ✓ | |
| *Anonymization and Pseudonymization* | | | | | | | | | ✓ | |
| **Data Portability** | ✓ | | | | ✓ | | | | ✓ | |
| **Doxxing** | | | ✓ | | | | | | | |

## Cybersecurity and Data Breaches

**90% of APAC DPAs have prioritized combating cyber threats and responding to data breaches in their strategy documents and regulatory actions throughout 2023 and 2024.**

- Some jurisdictions, such as Australia, Singapore and New Zealand, have established mandatory data breach notification schemes, while others, such as Hong Kong SAR and Malaysia, are still in the process of developing or implementing such requirements.
- Enforcement approaches differ significantly, with authorities like Australia's OAIC and Singapore's PDPC being more active in imposing penalties for data breaches, whereas others, such as Japan's PPC, lean more towards providing guidance and corrective actions. Authorities in certain jurisdictions adopt a proactive stance in investigating and addressing data breaches, particularly those in the high-priority group, while others are more reactive. The level of guidance provided to organizations also varies, with Hong Kong's PCPD offering detailed

guidelines, in contrast to more general advice given by others. Further, some authorities, like Japan's PPC, focus specifically on breaches within critical sectors such as healthcare and finance.

- DPA approaches to providing public information on data breaches also vary across the region. For instance, Australia's OAIC publishes regular reports on data breach notifications, whereas other authorities may provide less public information.

These differences reflect diverse regulatory approaches, varying stages of development in data protection regimes, and different assessments of the risks posed by data breaches across jurisdictions. As cyber threats continue to evolve, and with the occurrence of major data breaches, we anticipate that the prioritization of this area may increase uniformly across all jurisdictions.

| Priority Level | Jurisdiction |
|---|---|
| **High Priority** | **Australia**: The OAIC has made data breaches a key priority. It has been actively enforcing the Privacy Act's Notifiable Data Breaches scheme and responding to significant data breaches, such as the 2023 Latitude Financial data breach: the largest cyberattack on an Australian company to date. Notably, in 2023, the OAIC also initiated civil penalty proceedings against Australian Clinical Labs following a major data breach, further demonstrating a commitment to enforcement in this area. |
| | **Japan**: The PPC has prioritized responding to data breaches through the APPI's security and data breach notification requirements. The PPC has issued corrective recommendations and guidance to organizations following significant breaches in 2023 and 2024, demonstrating an active approach to enforcement in this area. |
| | **Singapore**: The PDPA imposes obligations to secure personal data and report certain data breaches. The PDPC's enforcement actions in 2023-24 have primarily concerned the former, and some of its largest fines to date have been imposed for failing to protect personal data from unauthorized access. |
| | **South Korea**: The PIPA has mandatory requirements to secure personal data and report certain data breaches. While responding to data breaches is not identified as a key priority in the PIPC's strategy documents, the PIPC has imposed significant fines for major data breaches throughout 2023 and 2024. |
| **Moderate Priority** | **Hong Kong SAR**: Though the PDPO does not include mandatory data breach reporting requirements, the PCPD has shown an increased focus on data breaches. In 2023, it updated its Guidance Note on Data Breach Handling and Data Breach Notifications, providing more detailed information on steps to be taken when handling a data breach. |

| | |
|---|---|
| | **New Zealand**: The OPC has made data breach response a priority, particularly since the introduction of mandatory breach reporting in the Privacy Act 2020. It has been actively working on implementing and enforcing these new provisions. |
| | **Philippines**: The NPC has been responsive to major data breaches, with its Complaints and Investigation Division proactively addressing several significant security incidents in 2023 and 2024. It has also established a formal Data Breach Notification Management System. |
| **Limited or Evolving Priority** | **China**: While the CAC has enforcement powers related to data breaches, responding to cyber threats and data breaches does not appear to be their highest priority compared to other areas. |
| | **Malaysia**: The latest amendments to Malaysia's PDPA that establish a mandatory data breach reporting framework. Operationalizing this framework is likely to be a key priority for the PDPD going forward. |
| | **Thailand:** As a newly established authority, Thailand's PDPC is still developing its approach to various aspects of data protection. While it has issued regulations on data breach notification, it is not clear whether responding to cyberthreats and data breaches is currently a top strategic priority. |

## Cross-Border Data Transfers

**80% of APAC DPAs have prioritized cross-border data transfers in their strategy documents and regulatory actions throughout 2023 and 2024.** However, they exhibit diverse priorities and approaches.

- Some jurisdictions, like China and South Korea, are actively working to operationalize their cross-border data transfer frameworks, with China notably introducing specific regulations for such transfers.
- International engagement varies, with Japan and Singapore taking a leading role in international initiatives, while others focus more on bilateral cooperation or participation in existing frameworks. Japan, in particular, is actively pursuing mutual adequacy decisions with other countries, a strategy not widely emphasized by all jurisdictions. The emphasis on international certification systems, such as the Global Cross-Border Privacy Rules (CBPR) also differs, with Japan and Singapore actively promoting these systems, while others may prioritize different mechanisms.
- In addition, China, Japan, Singapore, and Thailand have focused on promoting the use of contractual clauses for cross-border data transfers.

These variations reflect differing policy priorities and positions in the global digital economy, and assessments of the risks and opportunities associated with cross-border data flows. As digital trade and global data flows grow in importance, priorities in this area are likely to continue evolving.

| Priority Level | Jurisdiction |
|---|---|
| **High Priority** | **China**: The CAC has made cross-border data transfers a significant focus area. Throughout 2023 and 2024, it has issued detailed regulations and guidelines to operationalize the PIPL's cross-border data transfer framework, including the publication of the "Standard Contract Measures for the Export of Personal Information." |
| | **Japan:** Cross-border data transfers are a key priority for Japan's PPC. Their 2024 Activity Policy and International Strategy heavily emphasize promoting "Data Free Flow with Trust" (DFFT). The PPC is actively working on developing adequacy frameworks with other jurisdictions, promoting international certification systems (especially the Global CBPR system), and introducing model contractual clauses (MCCs) for global use. Japan has also established mutual adequacy decisions with the EU and UK. |
| | **Singapore**: The PDPC and IMDA actively engage in international cooperation on cross-border data flows. The IMDA has been appointed deputy chair of the Global CBPR Forum and has been instrumental in developing and promoting ASEAN-level guidance on cross-border data transfers, including a comparison between the EU's Standard Contractual Clauses and the ASEAN MCCs. |
| | **South Korea**: The PIPC's strategy documents identify cross-border data transfers as a key priority. Since late 2023, the PIPC has been working to operationalize recent amendments to the PIPA that introduced new legal bases for such transfers, including to jurisdictions with adequate protection levels or by certified controllers, and empowered the PIPC to suspend transfers that breach the PIPA. Notably, the PIPC has also established an Overseas Transfer Expert Committee to advise on these matters. It is also notable that South Korea has developed its own certification system (ISMS-P)[4] for cross-border data transfers. |
| **Moderate Priority** | **Hong Kong SAR**: The PCPD has been working with the CAC on a unique cross-border data transfer framework for transfers between Hong Kong SAR and nine cities in Guangdong. |
| | **New Zealand**: While not a top priority, cross-border data transfers are an area of focus for the OPC. New Zealand recently had its EU adequacy status reaffirmed, highlighting the importance of this issue. |

[4] https://www.pipc.go.kr/eng/user/lgp/bnp/certification.do

| | |
|---|---|
| | **Thailand**: The PDPC has issued regulations on cross-border data transfers that operationalize provisions under the PDPA. This includes guidance on use of the ASEAN MCCs. |
| **Limited or Evolving Priority** | **Malaysia**: The latest amendments to Malaysia's PDPA that overhaul the PDPA's cross-border data transfer framework. Operationalizing this framework is likely to be a key priority for the PDPD going forward. |

## Artificial Intelligence (AI)

**70% of APAC DPAs have prioritized AI governance and regulation in their strategy documents and regulatory actions throughout 2023 and 2024.** This is unsurprising, considering that the emergence of modern generative AI systems during this period garnered global attention and prompted DPAs in other regions to take major enforcement actions, such as the Italian DPA's decision in March 2023 to suspend ChatGPT from processing personal data in Italy.[5]

- Some jurisdictions (such as China, Singapore, and South Korea) have developed comprehensive policy frameworks and regulations specifically for AI, while others (such as Hong Kong SAR and Japan) have focused more on issuing guidelines or addressing AI within existing regulatory structures.
- Within the high-priority group, Singapore and South Korea have both been proactive in developing AI-specific policies, including releasing new voluntary frameworks and establishing regulatory sandboxes to promote responsible innovation. By contrast, China has focused on hard regulation, swiftly enacting binding regulations that target specific AI applications such as deepfakes and generative AI.
- Additionally, high-priority jurisdictions have allocated significant resources to AI governance, establishing dedicated teams or committees, signaling a higher level of commitment to this area.

These differences reflect varying levels of technological advancement, differing regulatory philosophies, and the perceived urgency of AI-related privacy issues across these jurisdictions. Given the rapidly evolving AI landscape, it is likely that priorities in this area will shift quickly in response to technological advancements and emerging challenges.

| Priority Level | Jurisdiction |
|---|---|
| **High Priority** | **China**: The CAC has been rapidly developing AI regulations, focusing on deepfakes and generative AI. It has enacted three legal instruments regulating specific AI technologies, including algorithmic recommendations, synthetic media, and generative AI. The CAC has also established registration frameworks for AI algorithms and generative AI services. |

[5] https://fpf.org/blog/how-data-protection-authorities-are-de-facto-regulating-generative-ai/

| | |
|---|---|
| | **Singapore:** AI governance has been a long-standing and key priority for Singapore's IMDA and the PDPC through forward-thinking initiatives such as the Model AI Governance Framework and AI Verify. In 2023-2024, the IMDA and PDPC expanded their focus to include generative AI, releasing a Model AI Governance Framework for Generative AI and launching several AI-related initiatives like the AI Verify Foundation and a Generative AI Evaluation Sandbox. The PDPC also issued a set of Advisory Guidelines on the use of personal data in AI recommendation and decision systems in March 2024. |
| | **South Korea:** The PIPC has adopted a proactive stance towards AI governance. It released a structured policy on AI regulation, established an AI Privacy Team and a Public-Private Consultative Council for AI Privacy, and launched a Prior Adequacy Review System for AI-driven services. It is also developing standards for protecting personal data in AI development and deployment. |
| **Moderate Priority** | **Australia**: The OAIC has demonstrated engagement with AI-related issues, participating in joint statements with other DPAs on data scraping, as well as contributing to government consultations on responsible AI and guidance documents released with other Australian regulatory agencies through the Digital Platform Regulators Forum (DP-REG). |
| | **Hong Kong SAR**: The PCPD has been actively working on AI governance, publishing guidance on ethical AI development and use. They have also conducted compliance checks on organizations' AI practices and issued new guidance on personal data protection considerations when using AI systems, including generative AI. |
| | **Japan:** The PPC has shown increasing engagement with AI-related privacy issues. They have issued guidance documents on the use of generative AI services and provided targeted recommendations to OpenAI over processing of sensitive personal data by ChatGPT. |
| | **New Zealand:** The OPC has issued guidelines on complying with privacy principles when using AI systems, including generative AI. |

## Biometrics and Facial Recognition Technology (FRT)

**60% of APAC DPAs have prioritized regulation of the use of biometric data, including by FRT, in their strategy documents and regulatory actions throughout 2023 and 2024.** These DPAs demonstrate diverse priorities and approaches:

- Some jurisdictions, such as China and New Zealand, are taking proactive steps to regulate the use of biometric data by developing specific regulations or codes.
- There is a notable emphasis on FRT in several jurisdictions, including China, Japan, and Australia, reflecting its widespread use and the potential risks associated with it.
- The focus on biometric data use also varies between public and private sectors. For example, Japan has concentrated on public sector use in public spaces or for crime prevention, whereas other jurisdictions take a broader approach, encompassing both the public and private sectors.

As biometric technology continues to advance and new challenges emerge, the landscape of biometric data regulation is likely to evolve, leading to potential shifts in regulatory priorities.

| Priority Level | Jurisdiction |
|---|---|
| **High Priority** | **China**: The CAC has been actively developing regulations for biometric data, including drafting regulations that, if enacted, would impose strict rules on FRT use in the private sector, including prohibitions in certain contexts and registration requirements. |
| | **Japan**: The PPC has focused on regulating the use of FRT, particularly for crime prevention. It has released reports and guidance clarifying the application of data protection law to FRT use and updated its Q&A guidelines with provisions on facial recognition cameras. |
| | **New Zealand**: The OPC has made biometrics a key priority, actively working on developing a biometrics privacy code since November 2023. To date, the OPC has released an exposure draft of the code, proposing new rules for agencies involved in the collection or use of biometric data, including proportionality assessments and enhanced transparency obligations. |
| **Moderate Priority** | **Australia**: The OAIC has identified developing privacy protections for biometric data as a key priority. It has also engaged in enforcement actions related to the use of FRT. |
| | **South Korea**: While not as prominent as AI in their strategic priorities, South Korea's PIPC has indicated plans to develop regulations for the use of biometric data as part of their efforts to create a trusted environment for new technologies. |

## Protecting Children's Personal Data

**50% of APAC DPAs have prioritized protecting children's personal data in their strategy documents and regulatory actions throughout 2023 and 2024.** These DPAs demonstrate diverse priorities and approaches:

- Some jurisdictions, like China, have developed specific and comprehensive regulations dedicated to children's privacy, while others address it within existing data protection frameworks or through guidelines.
- The definition and approach to different age groups also vary, as seen in South Korea's "Eraser Service," which extends protections to individuals up to 29 years of age, broader than typical definitions of children or minors.
- Technological solutions are being explored in some jurisdictions, such as Singapore's focus on privacy-preserving age estimation techniques.
- The scope of protection differs, with some jurisdictions concentrating primarily on online environments, while others adopt a broader approach that includes both online and offline contexts. There are also differences in how jurisdictions balance protecting children's data with empowering them to make informed decisions about their personal information.

These variations reflect differing policy priorities, assessments of the risks faced by children in digital environments, and stages of digital adoption among young people across these jurisdictions. As digital engagement among children continues to rise, it is possible that more jurisdictions will prioritize children's privacy in the future.

| Priority Level | Jurisdiction |
|---|---|
| **High Priority** | **China**: Protecting children's personal data is a significant focus for the CAC. It has developed comprehensive regulations to protect minors online, which took effect in January 2024. These regulations cover various aspects such as content control, personal information safeguards, and age-appropriate digital experiences. The CAC has also launched campaigns to address key issues for protecting minors online. |
| **Moderate Priority** | **Japan**: The PPC has recognized the need for enhanced protection of children's personal data in its review of the APPI. While not a top priority, it is one of several areas that the PPC is exploring for potential amendments to the law. |
| | **New Zealand**: The OPC has shown a growing focus on children's privacy. It launched a Children and Young People's Privacy project in 2023 to assess the adequacy of current privacy safeguards for children and young people. |
| | **Singapore**: The PDPC has increasingly focused on the protection of children's data. It released advisory guidelines on protecting children's personal data in 2024. It has also launched innovation challenges to develop privacy-preserving age estimation solutions. |

| | |
|---|---|
| | **South Korea:** The PIPC released a detailed policy plan for protecting children's personal data in 2022, but appears to have been less active in this area throughout 2023 and 2024. The PIPC's main focus has been on giving effect to a right to be forgotten for children by developing an "Eraser Service" enabling children and young people to request removal of online content containing their personal data. |

## Enforcement

Enforcement is a cornerstone function of DPAs globally, serving as a crucial mechanism to ensure compliance with data protection laws and to protect individuals' privacy rights. All 10 of the APAC DPAs examined in this Report are vested with investigatory and enforcement powers under their respective data protection laws. These powers typically include the ability to conduct investigations, issue corrective orders, impose financial penalties, and in some cases, pursue criminal prosecutions.

However, the way these powers are exercised, and the emphasis placed on enforcement activities, varies significantly across the region. This variation is reflected in two key aspects of enforcement that warrant closer examination: (1) **the availability of publicly available information in approaches to enforcement**; and (2) **level of enforcement activity**. Examining these two aspects provides valuable insights into the effectiveness and impact of data protection enforcement across the APAC region.

### Availability of Information on Enforcement Approaches

The availability of publicly-available information on a DPA's approach to enforcing data protection law can significantly impact the predictability of the regulatory environment and the ability of organizations to align their data protection practices with regulatory expectations. The degree to which DPAs are open about their enforcement strategies, decision-making processes, and outcomes differs markedly. While the majority of APAC DPAs provide insights into their enforcement policies and/or recent enforcement actions, others offer limited public information.

| Availability of Information | Jurisdiction |
|---|---|
| **High** | **Australia**: The OAIC publishes detailed guidance on its enforcement approach, including a Privacy Regulatory Action Policy and a Guide to Privacy Regulatory Action. The OAIC also regularly publishes its enforcement decisions, providing clear insights into its interpretation and application of the Privacy Act. |
| | **Hong Kong SAR**: The PCPD publishes its complaint-handling policy and reports on notable enforcement actions. The PCPD also releases case notes of its decisions, providing guidance on its interpretation and application of the PDPO. |

| | |
|---|---|
| | **Japan**: The PPC publishes its Monitoring and Supervision Policy annually. It also provides enforcement statistics in its annual reports and publishes information on its enforcement actions. |
| | **New Zealand:** The OPC publishes its compliance and regulatory action policy and complaint-handling policy. It also releases case notes from enforcement decisions and provides information about significant cases. |
| | **Philippines:** The NPC publishes advisories, circulars, and notable enforcement decisions and resolutions on its website. |
| | **Singapore:** The PDPC is highly transparent about its enforcement approach. It publishes detailed Advisory Guidelines on Enforcement of Data Protection Provisions, which are regularly updated. The PDPC also consistently publishes its enforcement decisions, offering valuable insights into its interpretation of the PDPA. |
| | **South Korea**: The PIPC publishes guidelines on various aspects of the PIPA and provides some information on enforcement actions in its annual reports. It also issues press releases on major enforcement actions and regularly publishes casebooks of notable decisions in the previous year. |
| **Moderate** | **Thailand**: Despite being the newest operational DPA, Thailand's PDPC has begun enforcement actions and releases brief summaries of enforcement decisions. It has also begun publishing guidelines on the operation of its enforcement powers under the PDPA. |
| **Limited** | **China**: The CAC publishes rules of procedure for enforcement cases on its website. However, detailed information about specific enforcement actions is limited, and there is no regular publication of enforcement decisions. |
| | **Malaysia**: The PDPD publishes limited information about its enforcement actions. It provides a summary of compound offenses and prosecutions on its website, but detailed enforcement decisions or comprehensive guidance on enforcement approaches are not readily available. |

## Level of Enforcement Activity

The frequency and intensity of enforcement actions taken by the 10 DPAs also show considerable variation. This is perhaps unsurprising given the differences in their home jurisdictions' history, legal culture, and economic context, the maturity and resourcing of the DPAs, and the powers afforded to them by applicable data protection laws.

While these factors make a precise comparison challenging, it is still possible to identify broad trends:

- Some authorities demonstrate a proactive and robust approach to enforcement, regularly conducting investigations and imposing significant penalties. Others appear to take a more reactive stance or focus on softer enforcement mechanisms such as warnings and corrective recommendations.
- The severity of penalties and the readiness to impose them also vary, with jurisdictions like South Korea and Singapore imposing significant fines, while others, such as Japan, tend towards corrective recommendations, imposing penalties only occasionally, in exceptional circumstances.
- Enforcement capabilities are another factor. Whereas South Korea's PIPC received an increased budget to engage in enforcement actions against global tech companies,[6] Australia's OAIC[7] recently saw its funding cut in 2024.

| Level of Activity | Jurisdiction |
|---|---|
| **High** | **Singapore**: The PDPC has been highly active in enforcement, particularly focusing on organizations' obligation to protect personal data from unauthorized access. It regularly imposes financial penalties for data breaches and has issued some of its largest fines in response to major breaches. The PDPC also issues directions to infringing organizations and accepts voluntary undertakings. |
| | **South Korea**: The PIPC has shown increasing enforcement activity, imposing significant fines for data breaches and PIPA violations. It recently strengthened its enforcement capabilities, including securing a litigation budget for potential lawsuits against global tech companies. |
| **Moderate or Increasing** | **Australia:** The OAIC has been taking a more active enforcement stance, particularly in relation to data breaches and privacy violations by large tech companies. It has also initiated civil penalty proceedings in the Federal Court and has been issuing more privacy determinations. However, the OAIC's budget for 2024 was notably cut by 56% compared with the previous year, potentially limiting the OAIC's ability to pursue large enforcement actions going forward. |
| | **Japan:** The PPC has been increasingly active in enforcement, particularly in response to major data breaches. It typically uses a graduated approach, |

[6] See page 79 of this Report.
[7] See page 28 of this Report.

| | |
|---|---|
| | starting with guidance and recommendations before moving to binding orders. Key focus areas include cybersecurity, AI governance, and compliance with APPI principles. |
| | **Hong Kong SAR:** The PCPD has been focusing on enforcing anti-doxxing provisions introduced in 2021. It has conducted criminal investigations, arrest operations, and issued cessation notices to online platforms. Other focus areas include data breaches and compliance with PDPO principles. |
| | **New Zealand**: The OPC has been selectively active in enforcement, with a focus on conciliation and mediation for complaint resolution. They have the power to issue compliance notices and can refer cases to the Human Rights Review Tribunal. Recent focus areas include biometrics and data breaches. |
| **Lower/Unknown** | **China:** The CAC has broad enforcement powers and has been active in several areas. However, public information on the CAC's enforcement activity is limited. |
| | **Philippines**: The NPC has been developing its enforcement capabilities, recently amending its Rules of Procedure to enhance its investigatory powers. It has responded to major data breaches, but overall enforcement actions appear more limited compared to some other jurisdictions. |
| | **Malaysia**: The PDPD's enforcement actions appear to be primarily focused on registration of data processing under the PDPA. Detailed information about other enforcement priorities is limited. |
| | **Thailand:** As a newly established authority, Thailand's PDPC is still developing its enforcement approach. They have recently started taking enforcement actions, with their first decision issued in late 2023 concerning unauthorized use of personal data by an insurance company. |

# Part 2: Individual DPA Profiles

## Australia

According to its key strategy documents, the Office of the Australian Information Commissioner (OAIC)'s key priorities for 2024 are online platforms, social media and high privacy impact technologies; security of personal information; ensuring privacy safeguards in the Consumer Data Right; and timely proactive release of government information. The OAIC's regulatory actions in the last year also indicate that it is engaging more on data protection issues arising from emerging technologies, making submissions to Australian government consultations, and taking a more active enforcement stance.

### Background

The OAIC is Australia's independent national regulator for privacy under the Privacy Act 1988 and Freedom of information (FOI) under the Freedom of Information Act 1982.

Established on November 1, 2010, the OAIC integrated the previous regulatory authority, the Office of the Privacy Commissioner. From 2014 to 2023, the roles of Privacy Commissioner and FOI Commissioner were performed by a single Information Commissioner. However, the OAIC has since returned to its original three-commissioner structure.[8] On February 19, 2024, Elizabeth Tydd assumed the role of the FOI Commissioner, and on February 26, 2024, Carly Kind assumed the role of Privacy Commissioner.[9] Each will serve a term of 5 years.

**Privacy Act 1988**

The OAIC's main role under the Privacy Act is to investigate suspected interferences with privacy and may do so either in response to a complaint or on its own initiative. Following an investigation, the OAIC may dismiss it or make a determination requiring the respondent to take corrective action and/or pay compensation for loss or damage. For serious or repeated privacy interferences, the OAIC can seek civil penalties through the courts of up to the greater of AU$50 million (approximately US$33.7 million), 3 times the benefit obtained, or 30% of turnover. The OAIC outlines how it exercises these powers in its **Privacy Regulatory Action Policy**[10] and **Guide to Privacy Regulatory Action**.[11]

[8] https://www.oaic.gov.au/newsroom/oaic-says-appointment-of-new-commissioners-a-significant-step

[9] https://www.directory.gov.au/portfolios/attorney-generals/office-australian-information-commissioner/office-australian-information-commissioner

[10] https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/privacy-regulatory-action-policy

[11] https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action

In addition to its enforcement role, the OAIC is also responsible for

- Conducting privacy assessments of whether entities are complying with the Act.
- Directing entities to develop enforceable privacy codes or give the OAIC privacy impact assessments.
- Recognizing external dispute resolution schemes to handle certain privacy complaints.

**Competition and Consumer Act 2010**

The OAIC oversees the 13 privacy safeguards for Australia's data portability framework, the Consumer Data Right (CDR), established by 2020 amendments to the Competition and Consumer Act 2010 and Privacy Act. The CDR enables secure data sharing in designated sectors. These currently include banking and energy but are being expanded progressively to the retail energy, insurance, financial services, and retail telecoms sectors. The OAIC's functions and powers in relation to the CDR are set out in the CDR Privacy Safeguard Guidelines.[12] Together with the ACCC, the OAIC has also published a **Compliance and Enforcement Policy for the CDR**.[13]

**Digital Platform Regulators Forum (DP-REG)**

The OAIC is part of the Digital Platform Regulators Forum (DP-REG), established in March 2022, which brings together Australian federal regulators addressing digital issues, including the OAIC, eSafety Commission, Australian Competition & Consumer Commission (ACCC), and Australia Communications and Media Authority.[14]

## Overview of Key Strategic Documents

The OAIC's strategic priorities and planned initiatives are outlined in the following key documents:

- **Corporate Plan**: Released annually, this document highlights the OAIC's operating context, strategic priorities, and performance measurement approach for regulating privacy and information access in Australia. The latest Corporate Plan, published in August 2023, indicates that the OAIC's key activities in 2023 and 2024 are:
    - Influencing and upholding privacy and information access rights frameworks.
    - Advancing online privacy protections.
    - Encouraging proactive release of government-held information.
    - Taking a contemporary approach to regulation.[15]

- **OAIC Regulatory Priorities:** Published annually, this brief statement aligns with the key activities identified in the Corporate Plan. According to its latest statement, the OAIC's regulatory priorities for 2024 are:
    - Online platforms, social media, and high privacy impact technologies.
    - Security of personal information.
    - Ensuring privacy safeguards in the Consumer Data Right.
    - Timely proactive release of government information.[16]

---

[12] https://www.oaic.gov.au/consumer-data-right/consumer-data-right-guidance-for-business/consumer-data-right-privacy-safeguard-guidelines

[13] https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/compliance-and-enforcement-policy

[14] https://dp-reg.gov.au/

[15] https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/corporate-plans/corporate-plan-202324

[16] https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/oaic-regulatory-priorities

- **Annual Report:** The OAIC also publishes Annual Reports, which provide a statistical overview of complaints, inquiries, and data breach notifications received by the OAIC in the previous year. The latest Annual Report indicates that from 2022 to 2023, the OAIC handled 11,672 privacy enquiries, received 3,402 privacy complaints, and fielded 895 data breach notifications.[17] Leading sectors for breaches were health service providers, finance, recruitment agencies, insurance, and legal/accounting services.

## Key Priorities

The OAIC's strategic priorities for 2024, as outlined in the key documents and key regulatory actions by the OAIC in 2023 and 2024, focus on the following areas:

### Legal Reform

A major context for the OAIC currently is the ongoing review of the Privacy Act, which began in 2020 and culminated in a bill to amend the Act, the "Privacy and Other Legislation Amendment Bill 2024" (Bill), which was tabled in the House of Representatives on 12 September 2024.[18] Notably, the Bill only includes a subset of the proposed amendments endorsed by the Australian government in response to the Privacy Act review, published in September 2023.[19]

Provisions of the Bill that impact the OAIC's role include:

- A requirement for the OAIC to develop a Children's Online Privacy Code within 2 years of the Bill coming into force.
- Expanded monitoring and investigatory powers for the OAIC, including the power to conduct public inquiries.
- A tiered civil penalty regime that will allow the OAIC to tailor penalties based on the severity of the privacy infringement.

While the OAIC does not have the power to shape legislation directly, the OAIC actively engaged with the review process by making detailed submissions during the two main rounds of consultation in 2020[20] and 2021.[21]

### Enforcement

The OAIC's approach to enforcement has been largely consistent over the years. It generally opts for a conciliatory approach before progressing to formal enforcement. For instance, the OAIC's 2022-2023 Annual Report indicated that it handled 94% of 2022-23 complaints via conciliation.

However, the OAIC will use its formal powers where warranted and in recent years, has been taking a more active stance to enforcement. For instance, the OAIC finalized 17% more privacy complaints in 2022-2023 compared with

[17] https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/oaic-annual-reports/annual-report-2022-23
[18] https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r7249_first-reps/toc_pdf/24115b01.PDF
[19] https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report
[20] https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission
[21] https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-discussion-paper

2021-2022. In doing so, it issued nine privacy determinations. As of the date of this Report, the OAIC has issued 6 privacy determinations in 2024.[22]

The OAIC is also initiating civil penalty proceedings in Australia's Federal Court more often. It has been involved in proceedings against Facebook since 2020, following an investigation into Facebook's disclosure of Australians' personal data to Cambridge Analytica from March 2014 to May 2015.[23] These proceedings were initially held up over jurisdictional issues. In March 2023, however, the High Court of Australia permitted the case to proceed by granting the OAIC leave to serve legal documents on Facebook (now Meta) in the US.[24] In late 2023, the OAIC also commenced civil proceedings against Australian Clinical Labs following a major data breach (see below).

However, changes in the OAIC's budget suggest that its enforcement capacity in 2025-2025 will remain similar to that for previous years. While the 2023-2024 federal budget increased the OAIC's funding by 56% over the previous year, the 2024-2025 federal budget cut the OAIC's funding back to just above 2022-2023 levels.

## Biometrics and AI

As stated above, the OAIC has identified "**high privacy impact technologies**," such as facial recognition and AI, as an enforcement priority for 2024.

A key enforcement activity in this regard is the OAIC's ongoing action against U.S. company Clearview AI. In March 2020, the OAIC initiated an investigation into Clearview AI's scraping of facial images from social media to build a facial recognition tool. In October 2021, the OAIC issued a determination which found that Clearview AI had breached several obligations under the Privacy Act.[25] Clearview AI appealed the decision, claiming that it was not subject to the Privacy Act as it did not conduct business in Australia. On 8 May 2023, the Administrative Appeals Tribunal issued a decision in favor of the OAIC.[26] On 21 august 2024, the OAIC issued a statement confirming that the 2021 determination remains in effect and requires Clearview AI to cease collecting images and delete existing data previously collected from individuals in Australia.[27] The OAIC also indicated that it would take no further action against Clearview AI regarding the matter

[22] These include 'AGX' and 'AGY' (Privacy) [2024] AICmr 16 (29 January 2024); 'AHL' and TICA Default Tenancy Control Pty Ltd (Privacy) [2024] AICmr 26 (9 February 2024); 'AHM' and JFA (Aust) Pty Ltd t/a Court Data Australia (Privacy) [2024] AICmr 29 (12 February 2024); Rao Medical Centre (Privacy) [2024] AICmr 40 (23 February 2024); Cherrybrook Medical Centre (Privacy) [2024] AICmr 43 (28 February 2024). All OAIC determinations are available at https://classic.austlii.edu.au/au/cases/cth/AICmr/2024/

[23] https://www.hcourt.gov.au/cases/case_s137-2022

[24] https://www.oaic.gov.au/newsroom/high-court-clears-way-for-oaic-case-against-facebook-to-proceed

[25] https://www.oaic.gov.au/__data/assets/pdf_file/0016/11284/Commissioner-initiated-investigation-into-Clearview-AI,-Inc.-Privacy-2021-AICmr-54-14-October-2021.pdf

[26] https://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AATA/2023/1069.html

[27] https://www.oaic.gov.au/news/media-centre/statement-on-clearview-ai

The OAIC has been less proactive than other data protection authorities in the APAC region and other Australian regulators, such as the eSafety Commissioner,[28] in issuing guidance on the use of AI. To date, the OAIC has only published a set of guidelines on conducting data analytics in compliance with the Privacy Act, which were published in 2018.[29]

However, the OAIC increased its engagement on these issues in 2023.

- In August 2023, the OAIC joined eleven other data protection authorities globally in issuing a joint statement on data scraping and data protection.[30]
- In September 2023, the OAIC made a submission[31] to the Australian government's public consultation on regulatory options to support responsible AI in Australia.[32]

Further, the OAIC has contributed to the DP-REG's recent efforts to address new issues from advanced AI systems.

- In June 2023, the DP-REG published a working paper on harms and risks from algorithms used in content moderation, recommender systems, and targeted advertising.[33]
- In September 2023, DP-REG members made a joint submission to the Australian government's consultation responsible AI.[34]
- In November 2023, the DP-REG published a working paper on algorithms and large language models (LLMs).[35] The working papers outline the impacts, risks, and regulatory considerations of these technologies but are high-level in scope.

## Data Portability

While the OAIC and ACCC initially focused on educating consumers about the CDR and increasing industry participation, it is likely that these regulators will increasingly focus on enforcement going forward.

Notably, in October 2023, the OAIC and ACCC updated their joint Compliance and Enforcement Policy for the CDR to identify priority conduct that is likely to attract enforcement action. This conduct includes:

- hindering the CDR's operation;
- failing to meet compliance dates;
- insufficient data quality;
- inadequate oversight of third-party participants by accredited data recipients;
- insufficient security measures;
- misleading or deceptive conduct; and

[28] See, for example, the eSafety Commissioner's Tech Trends Position Statements on generative AI (August 2023) and recommender systems and algorithms (December 2022): https://www.esafety.gov.au/industry/tech-trends-and-challenges

[29] https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/guide-to-data-analytics-and-the-australian-privacy-principles

[30] https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf

[31] https://consult.industry.gov.au/supporting-responsible-ai/submission/view/506

[32] https://consult.industry.gov.au/supporting-responsible-ai

[33] https://dp-reg.gov.au/publications/working-paper-1-literature-summary-harms-and-risks-algorithms

[34] https://dp-reg.gov.au/news-and-media/digital-platform-regulators-make-joint-statement-ai

[35] https://dp-reg.gov.au/publications/working-paper-2-examination-technology-large-language-models

- misuse of CDR data.

## Cybersecurity

As stated above, the OAIC has identified enduring the security of personal data as a key priority in 2024. This priority likely reflects the fact that Australia experienced several major data breaches in the last year. These include the largest cyberattack on an Australian company, Latitude Financial, in March 2023 which compromised the financial data of 7.9 million individuals.

In February 2024, the OAIC published a report on data breach notifications received from July to December 2023. The report revealed a 19% increase in reported data breaches compared to the first half of 2023, identified malicious or criminal attacks as the leading source of data breaches, and noted that the health and finance sectors were the top reporters of data breaches.

In November 2023, the OAIC, for the second time in its history, initiated civil penalty proceedings against Australian Clinical Labs in Australia's Federal Court for serious interference with Australians' privacy.[36] The case concerned a 2022 cyberattack against Medlab Pathology, owned by Australian Clinical Labs (ACL), in which threat actors exfiltrated the personal data of at least 223,269 individuals.[37] The OAIC commenced investigations into the breach in December 2022[38] and alleged that ACL had:

- seriously interfered with the privacy of 21.5 million individual by failing to protect their personal data, in breach of the Privacy Act;
- failed to promptly assess a suspected data breach; and
- delayed notifying the OAIC about the breach.

## International Cooperation

The OAIC is a member of the Global Privacy Assembly,[39] and the Asia Pacific Privacy Authorities (APPA) Forum.[40] It has also signed memoranda of cooperation with DPAs in the UK,[41] Ireland,[42] and Singapore.[43]

[36] https://www.oaic.gov.au/newsroom/oaic-commences-federal-court-proceedings-against-australian-clinical-labs-limited
[37] https://www.oaic.gov.au/__data/assets/pdf_file/0017/112526/AIC-v-Australian-Clinical-Labs-Limited-concise-statement.pdf
[38] https://www.oaic.gov.au/newsroom/oaic-opens-investigation-into-medlab-over-data-breach
[39] https://globalprivacyassembly.org/participation-in-the-assembly/list-of-accredited-members/
[40] https://www.appaforum.org/members/
[41] https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/memorandums-of-understanding/current-memorandums-of-understanding/mou-with-the-information-commissioner-for-the-united-kingdom
[42] https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/memorandums-of-understanding/current-memorandums-of-understanding/mou-with-the-data-protection-commissioner-of-ireland
[43] https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/memorandums-of-understanding/current-memorandums-of-understanding/mou-with-the-personal-data-protection-commission-of-the-republic-of-singapore

The OAIC publishes an international engagement strategy but has not updated it since 2021.[44] Key international engagements in 2023 and 2024 include signing on to a joint statement by multiple data protection authorities against data scraping (see above) and pursuing a joint investigation into the Latitude Financial data with New Zealand's privacy authority.[45]

[44] https://www.oaic.gov.au/__data/assets/pdf_file/0017/6506/oaic-international-strategy.pdf
[45] https://www.oaic.gov.au/newsroom/joint-australianew-zealand-investigation-into-latitude-group

# China

A survey of recent regulatory actions by the Cyberspace Administration of China (CAC) reveals that its priority areas throughout 2023 and 2024 have been rulemaking around AI (particularly generative AI), children's privacy, and cross-border data transfers. These actions reflect a focus on managing the risks and opportunities presented by emerging technologies, particularly AI and facial recognition, maintaining security requirements while also strengthening protections for vulnerable groups such as minors. Key areas to watch going forward include the further implementation of AI regulations and finalization of rules around facial recognition. However, the CAC has also demonstrated that it can respond quickly in issuing regulations to address specific challenges from emerging technologies, so it is always possible that the CAC will release new regulations as the technology landscape develops.

## Background

China's primary data protection law is the Personal Information Protection Law (PIPL), which took effect in November 2021.[46] Notably, the PIPL did not establish a dedicated data protection authority and instead, assigned administrative responsibility for enforcing the PIPL to China's pre-existing cyberspace regulator, the CAC.

The CAC[47] was established in 2014 and is the central authority for regulating online activity and cybersecurity. In addition to enforcing the PIPL, the CAC also enforces China's other keystone cyber laws: the Cybersecurity Law (CSL) and the Data Security Law (DSL). The CAC operates under the direct control of the Central Commission for Cybersecurity and Informatization (CCCI), a high-level group led by President Xi Jinping. It is organized into over a dozen bureaus with specialized functions with a core executive team consisting of a Director and four Deputy Directors.[48] The current director is Zhuang Rongwen (since 2015),[49]

As with other administrative bodies in China, the CAC has a central office in Beijing and is responsible for coordinating cyberspace and informatization policy at the national level. The CAC also has 32 offices at the provincial and city levels, with potentially more departments on lower levels.

Notably, the CAC is empowered to draft and implement legally binding rules within its areas of competence, which include content moderation, cyber and data security, informatization, and personal data protection. These rules can take any of the following forms

- **Regulations** (条例): Comprehensive and systematic rules covering particular aspects of administrative work.

[46] https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm. English translation available at http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm
[47] https://www.cac.gov.cn/
[48] https://www.cac.gov.cn/wxzw/bgs/bld/A09370101index_1.htm
[49] https://www.cac.gov.cn/wxzw/bgs/bld/zrw/A0937010101index_1.htm

- **Provisions** (规定): Partial regulations covering specific aspects of administrative work.
- **Measures** (办法): Specific rules focusing on narrow items of administrative work, such as a subset of a policy area.

The CAC is granted broad powers to investigate and enforce potential breaches of the PIPL and other relevant laws. Under the PIPL, the CAC may impose penalties of up to 1 million yuan (approximately US$139,400) and can also order corrections and suspension or even termination of services. While information about its enforcement decisions is limited, the CAC publishes its rules of procedure for enforcement cases on its website, with the latest version released in March 2023.[50]

## Overview of Key Strategic Documents

The CAC does not publish comprehensive strategy documents. However, its official website regularly features updates on the CAC's activities at the national and provincial levels, with dedicated sections on policies and regulations,[51] internet content management,[52] cybersecurity,[53] data governance,[54] informatization,[55] and international cooperation.[56]

## Key Priorities

### AI

#### Rulemaking

Over the past few years, the CAC has been rapidly developing AI regulations, focusing on deepfakes and generative AI. This work has positioned China as one of the first major global economies to establish a dedicated regulatory framework in this area.

To date, the CAC has enacted three legal instruments that each regulate specific AI technologies.

**Provisions on the Management of Algorithmic Recommendations in Internet Information Services (Algorithmic Recommendation Provisions)**
**(互联网信息服务算法推荐管理规定)**[57]
The Algorithmic Recommendation Provisions were enacted in November 2021 and took effect in March 2022. These Provisions impose binding obligations on service providers who use algorithmic recommendation

[50] http://www.cac.gov.cn/2023-03/23/c_1681211418907384.htm
[51] https://www.cac.gov.cn/wxzw/zcfg/A093703index_1.htm
[52] https://www.cac.gov.cn/wxzw/hlwnrgl/A093704index_1.htm
[53] https://www.cac.gov.cn/wxzw/wlaq/A093705index_1.htm
[54] https://www.cac.gov.cn/wxzw/sjzl/A093708index_1.htm
[55] https://www.cac.gov.cn/wxzw/xxh/A093706index_1.htm
[56] https://www.cac.gov.cn/wxzw/gjjl/A093707index_1.htm
[57] https://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm

technology in providing online services within the People's Republic of China (PRC). Key obligations include managing security, assessing algorithms, providing transparency and "opt-outs" to users, and establishing complaint handling procedures. Notably, the Provisions also prohibit use of recommendation algorithms for certain purposes, such as promoting illegal activities, disseminating fake news or misinformation, engaging in anti-competitive behavior, endangering the health and wellbeing of minors, and engaging in discriminatory practices.

**Regulations on the Administration of Deep Synthesis of Internet Information Technology (Deep Synthesis Regulations)**
**(互联网信息服务深度合成管理规定)**[58]
The Deep Synthesis Regulations were enacted in November 2022 and took effect in January 2023. These Regulations apply to AI-generated synthetic media transmitted over the Internet. The Regulations mainly govern providers of online services that use AI technology to generate or edit content (deep synthesis service providers). However, they also outline obligations for: (1) third parties who provide technical support to deep synthesis service providers (e.g., cloud service providers); (2) app stores and other distribution platforms; and (3) users of deep synthesis services. Generally, these obligations aim to avoid the spread of misinformation and manipulation of public opinion online – for instance by requiring AI-generated content to be watermarked.

**Interim Measures for the Management of Generative AI Services (Interim Generative AI Measures)**
**(生成式人工智能服务管理暂行办法)**[59]
The Interim Generative AI Measures were enacted in May 2023 and took effect in August 2023. These Measures apply to providers of services that: (1) use AI to generate content; and (2) are offered to the public in the PRC (generative AI service providers). Unlike the Deep Synthesis Regulations, the Interim Generative AI Measures only impose obligations on service providers.

The Interim Generative AI Measures are the most comprehensive of the three legal instruments and notably, apply not only to provision of services but also training of generative AI models. Key obligations include, among others:

- only using training data and generative AI models from "lawful sources;"
- obtaining consent for processing of personal data when training model;
- limiting excessive collection of personal data;
- requiring anonymization or pseudonymization of input information and records;
- watermarking AI-generated content; and
- establishing systems for receiving and addressing complaints and incident reports.

## Registration of AI Services

Notably, the Algorithmic Recommendation Provisions, Deep Synthesis Regulations, and Interim Generative AI Measures all require service providers to register with the CAC if their services are capable of altering public

[58] https://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm
[59] https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

opinion or mobilizing the public. The CAC opened an online registration portal[60] in February 2022, and since then, has been actively processing registrations and publishing lists of approved algorithms and AI models. As of August 2024, 44 recommendation algorithms,[61] 487 different deep synthesis algorithms and models[62] and 188 generative AI services[63] have been successfully registered with the CAC.

## Biometrics

The CAC is currently developing a set of regulations on use of facial recognition technologies (FRT). From August to September 2023, it consulted on a draft "**Regulations on Security Management for Facial Recognition Technology Applications**" (人脸识别技术应用安全管理规定 (试行) (征求意见稿), henceforth: Draft FRT Regulations).[64] If enacted in their current form, the Draft FRT Regulations in China would prohibit all entities in the PRC to refrain from using FRT if equally effective alternatives exist and from deploying FRT in private spaces and for purposes like identity verification (unless legally required). Such entities would also be required to obtain consent, provide public notices, conduct impact assessments, and minimize data collection. Those using FRT in public spaces or storing over 10,000 facial records would also be required to register with the local CAC branch within 30 working days and report any significant changes in FRT deployment. The status of the Draft FRT Regulations is uncertain as the CAC has not provided any further updates since the initial consultation.

## Children's Privacy

Throughout 2023 and 2024, the CAC has developed comprehensive regulations to protect minors online, focusing on content control, personal information safeguards, and age-appropriate digital experiences.

A key initiative in this regard is the development of the "**Regulations on the Protection of Minors in Cyberspace**" (未成年人网络保护条例),[65] which were enacted in October 2023 and took effect in January 2024. These Regulations apply to schools, parents and guardians, and businesses involved in online activities related to minors. They build on existing children's privacy provisions in the PIPL by, among others, requiring online platforms to implement age verification, establish convenient mechanisms for minors or their guardians to exercise their data subject rights under the PIPL, and various security controls, including limiting employees' access to minors' data. However, the Regulations also focus on broader issues such as promoting internet literacy for minors, content moderation, and combating internet addiction.

On the same day that the Regulations took effect, the Beijing branch of the CAC launched a 3-month campaign to address key issues for protecting minors online, such as harmful content, online bullying, privacy protection, and internet addiction.[66]

[60] https://beian.cac.gov.cn/#/index
[61] https://www.cac.gov.cn/2022-08/12/c_1661927474338504.htm
[62] https://www.cac.gov.cn/2024-08/05/c_1724541639039621.htm
[63] https://www.cac.gov.cn/2024-04/02/c_1713729983803145.htm
[64] http://www.cac.gov.cn/2023-08/08/c_1693064670537413.htm
[65] https://www.cac.gov.cn/2023-10/24/c_1699806932316206.htm
[66] http://bj.people.com.cn/n2/2023/1230/c233088-40698920.html

Additionally, in August 2023, the CAC consulted on a set of draft "**Guidelines for the Construction of a 'Minor Mode' for Mobile Internet**" (移动互联网未成年人模式建设指南 (征求意见稿)).[67] These draft Guidelines seek to combat internet addiction and create a safer online environment for minors by outlining specifications for a "minor mode" – a simplified user interface that would automatically activate when a minor uses a mobile device, application, or app store. The interface would only display age-appropriate content to minors, restrict their access to other online information and services, and warn them and their parents about the risk of internet addiction.

## Cross-Border Data Transfers

When enacted in 2021, the PIPL introduced a structured framework for transfers of personal data out of the PRC in which the CAC plays an integral role. This framework recognizes four mechanisms for transferring personal data out of the PRC: (1) passing a security assessment by the CAC; (2) undergoing certification by a CAC-approved body; (3) entering into an agreement the recipient of the data, using standard contractual clauses (SCCs) issued by the CAC; or (4) meeting other conditions provided in laws or regulations or required by the CAC.

Building on the foundation in the PIPL, the CAC has been refining this framework by issuing regulations and guidelines that ensure that organizations are able to rely on these mechanisms. Throughout 2022, the CAC issued guidelines on the security assessment and certification mechanism. In February 2023, the CAC enacted "**Measures on the Standard Contract for the Cross-Border Transfer of Personal Information**" (个人信息出境标准合同办法).[68] These Measures took effect in June 2023 but provided a 6-month grace period for organizations to comply with them. The Measures provided necessary information for organizations to rely on the SCC mechanism under the PIPL, including a set of standardized terms for data exporters to use in contracts with overseas recipients, and clarifications around filing requirements. Notably, the Measures require data exporters to file a copy of the signed contract and an impact assessment, together with other prescribed documents, with a local CAC branch. In May 2023, the CAC also released guidelines providing further details on the filing process for SCCs.[69]

Throughout end-2023 and 2024, the focus of the CAC's rulemaking shifted from operationalizing the PIPL framework to facilitating cross-border data transfers by further clarifying, and in some cases, loosening requirements.

In March 2024, the CAC released its "**Regulations on Promoting and Standardizing Cross-Border Data Flows**" (促进和规范数据跨境流动规定),[70] which took effect immediately. Key provisions include:

- Clarifying that CAC security assessments are only required for transfers involving:
    - "important data;"
    - personal data of more than 1 million individuals or sensitive personal data of more than 10,000 individuals;

[67] https://www.cac.gov.cn/2023-08/02/c_1692541991073784.htm
[68] https://www.cac.gov.cn/2023-02/24/c_1678884831596384.htm
[69] https://www.cac.gov.cn/2023-05/30/c_1687090906222927.htm
[70] https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm

- critical infrastructure operators.

- Exempting certain data transfers from compliance requirements, including
  - Data related to international trade, cross-border transportation, academic cooperation, etc.
  - Data collected or generated outside China;
  - Personal data transferred for contractual obligations or human resource management;
  - Personal data transferred in emergencies to protect life, health, or property; and

- Empowering China's 21 Pilot Free Trade Zones[71] to create their own exemptions from the CAC's default transfer requirements.

Further, in December 2023, the CAC and Hong Kong's Innovation, Technology and Industry Bureau released guidelines[72] for implementing standard contracts for cross-border data flows within the so-called Greater Bay Area (GAB), which spans nine cities in Guangdong Province as well as China's two Special Administrative Regions (SARs), Hong Kong SAR, and Macao SAR. These guidelines introduce a new set of SCCs with relaxed requirements for transfers within the GBA, including removing volume limits on personal data transfers (except for "important data"), and simplifying documentation and filing processes.

[71] See https://www.tradecommissioner.gc.ca/china-chine/ftz-zle.aspx?lang=eng
[72] https://www.cac.gov.cn/2023-12/13/c_1704042786237103.htm

# Hong Kong SAR

The Office of the Privacy Commissioner for Personal Data (PCPD), established under the Personal Data (Privacy) Ordinance (PDPO), is the statutory body responsible for safeguarding personal data privacy in Hong Kong.

The PCPD's key priorities for 2024, as outlined in its strategic documents and recent regulatory actions, include combatting doxxing, studying the impact of AI on personal data, and fostering international cooperation on data protection issues. The PCPD is also working with the Hong Kong government to review and propose amendments to the PDPO, aiming to strengthen personal data protection and address challenges posed by emerging technologies.

## Background

Hong Kong's primary data protection law, the PDPO, came into effect in December 1996.[73] The PDPO sets out Data Protection Principles (DPPs) that govern how data users may lawfully collect, use, and disclose personal data.

The PDPO has undergone two major rounds of amendments since its enactment. Major amendments to the PDPO in 2012 introduced provisions on direct marketing and enhanced protection against new privacy challenges.[74] Further amendments in 2021 aimed to combat doxxing.[75]

The PCPD,[76] established under Section 5 of the PDPO, is responsible for enforcing the PDPO. The PCPD is led by a Privacy Commissioner, who is appointed by the Chief Executive of Hong Kong for a five-year term and supported by three Assistant Privacy Commissioners.[77] The current Commissioner is Ada Chung (since 2020).[78]

Section 8 of the PDPO empowers the PCPD with investigatory and enforcement powers and mandates the publication of best practices and guidance for organizations and the general public. The Privacy Commissioner generally promotes conciliation to resolve disputes between data subjects and complained parties. Where complaints involve criminal elements or cannot be conciliated, the PCPD may carry out investigations and issue warnings or enforcement notices for PDPO contraventions. Non-compliance with enforcement notices is a criminal offense, attracting fines up to HK$100,000 (approximately US$12,800) and imprisonment for up to two years.

[73] https://www.elegislation.gov.hk/hk/cap486
[74] https://www.pcpd.org.hk/english/data_privacy_law/amendments_2012/amendment_2012.html
[75] https://www.pcpd.org.hk/english/data_privacy_law/amendments_2021/amendment_2021.html
[76] http://www.pcpd.org.hk/
[77] https://www.pcpd.org.hk/english/about_pcpd/our_organisation/staff/executive_staff.html
[78] https://www.pcpd.org.hk/english/about_pcpd/commissioner/commissioner_bio.html

The PCPD publishes its complaint handling policy,[79] reports on notable enforcement actions,[80] and case notes of its decisions,[81] offering guidance on its interpretation and application of the PDPO.

## Overview of Key Strategic Documents

The PCPD's high-level strategies and goals are published on its website, focusing on enforcement, compliance monitoring, awareness promotion, corporate governance, and monitoring technology and data protection trends.[82] More specific strategy documents include:

- **Reports to the Legislative Council**: On February 19, 2024, the PCPD presented a paper, titled "**Report on the Work of the Office of the Privacy Commissioner for Personal Data in 2023**" (Panel Paper), to the Legislative Council Panel on Constitutional Affairs. The Panel Paper details the PCPD's work in 2023 and outlines its strategic focus areas for 2024.[83]
- **Annual Reports:** Schedule 2 of the PDPO requires the Commissioner to publish an annual report detailing the activities of the Commissioner during that year, including a general survey of developments. On November 8, 2023, the PCPD published its annual report for 2022-23," titled "**Protecting Personal Data Privacy for a Smart Hong Kong - 2020-23**." (Annual Report).[84]

## Key Priorities

### Legal Reforms

The PCPD and the Hong Kong government have been actively working to review the PDPO since February 2023.[85] In its Panel Paper, the PCPD highlighted several areas for potential amendments, including:

1. Establishing a mandatory data breach notification mechanism.
2. Requiring data users to devise a data retention period policy.
3. Empowering the Privacy Commissioner to impose administrative fines.
4. Directly regulating data processors.
5. Clarifying the definition of personal data.

No timeline has been provided on when legislation will be tabled to enact these proposed amendments.

### Doxxing

Combatting doxxing is a key strategic focus for the PCPD in 2024, as highlighted in the Panel Paper. The PCPD has prioritized enforcing the PDPO's anti-doxxing provisions since they were enacted in 2021. From October 2021 to December 2023, the PCPD commenced criminal investigations for 254 doxxing cases, conducted 42 arrest

[79] https://www.pcpd.org.hk/english/complaints/policy/complaint_policy.html
[80] https://www.pcpd.org.hk/english/enforcement_reports/report.html
[81] https://www.pcpd.org.hk/english/enforcement/case_notes/casenotes.php
[82] https://www.pcpd.org.hk/english/about_pcpd/our_role/what_we_do.html
[83] https://www.legco.gov.hk/yr2024/english/panels/ca/papers/ca20240219cb2-157-2-e.pdf
[84] https://www.pcpd.org.hk/english/resources_centre/publications/annual_report/annualreport2023.html
[85] https://www.legco.gov.hk/yr2023/english/panels/ca/papers/ca20230220cb2-132-2-e.pdf

operations, and issued 1,878 cessation notices to 41 online platforms, requesting the removal of over 28,300 doxxing messages. The overall compliance rate for removing doxxing messages has been over 95%. It is likely that enforcing these provisions will remain a key priority for the PCPD going forward.

## AI

Emerging technologies, particularly AI, are a key strategic focus for the PCPD in 2024. The Panel Paper notes the PCPD's plans to conduct in-depth studies and engage with stakeholders to assess AI's impact on personal data privacy.

From August 2023 to February 2024, the PCPD carried out compliance checks on 28 local organizations' collection, use, and processing of personal data for AI development and use, as well as their AI governance structures.[86] The PCPD found that most organizations use AI in their daily operations and have established internal AI governance frameworks, but only a few collect personal data through AI products and services. It also found that organizations using AI in their daily operations had implemented appropriate security measures and conducted privacy impact assessments before developing or deploying AI products and services. As a result, the PCPD found no contraventions of the PDPO among the reviewed organizations.

In June 2024, the PCPD followed up on the compliance checks by publishing a new set of guidance on the using AI systems, including generative AI, in compliance with local data protection laws.[87] The guidance, titled "**Artificial Intelligence: Model Personal Data Protection Framework**,"[88] (Model PDP Framework) builds on the PCPD's previous AI guidance, such as the "**Guidance on the Ethical Development and Use of Artificial Intelligence**" (2021)[89] and "**10 TIPS for Users of AI Chatbots**" (2023).[90]

The Model PDP Framework focuses on four key areas: (1) AI Strategy and Governance; (2) Risk Assessment and Human Oversight; (3) Customization of AI Models; and (4) Communication with Stakeholders. Broadly, it emphasizes the importance of ethical AI use, establishing robust governance structures, adopting risk-based approaches, ensuring good data governance, and maintaining transparency with stakeholders. It also provides guidance on procuring AI solutions.

The Panel Paper also recognizes data scraping for training generative AI as a global issue and intends to engage with social media platforms to address related concerns. Notably, the PCPD joined 11 other data protection authorities in signing a joint statement on data scraping and the protection of privacy in August 2023.[91]

[86] https://www.pcpd.org.hk/english/news_events/media_statements/press_20240221.html
[87] https://www.pcpd.org.hk/english/news_events/media_statements/press_20240611.html
[88] https://www.pcpd.org.hk/english/resources_centre/publications/files/ai_protection_framework.pdf
[89] https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_ethical_e.pdf
[90] https://www.pcpd.org.hk/english/resources_centre/publications/files/ai_chatbot_leaflet.pdf
[91] https://www.pcpd.org.hk/english/news_events/media_statements/press_20230825.html

## Data Breach Notification

Though the PDPO does not currently contain mandatory data breach notification requirements, responding to data breaches will likely be a priority area for the PCPD in 2024. The Panel Paper indicates that in the preceding year, there was nearly a 50% increase in data breach notifications, rising from 105 in 2022 to 157 in 2023.

In June 2023, the PCPD issued an updated Guidance Note on Data Breach Handling and Data Breach Notifications,[92] providing more granular information on the steps to be taken when handling a data breach compared to the 2019 version.[93] The PCPD also offers an online form for organizations to notify data breaches, although there is currently no legal obligation under the PDPO to do so.[94]

## Cross-Border Data Transfers

The PDPO contains a framework for cross-border data transfers. However, the relevant provisions are not operational as of August 2024, and there are no indications as to when the PCPD plans to implement them. To date, the PCPD has released a set of non-binding guidelines on cross-border data transfers,[95] and a set of existing Recommended Model Clauses (RMCs).[96]

In December 2023, China's CAC released a new voluntary Standard Contract for the Cross-boundary Flow of Personal Information within the Guangdong-Hong Kong-Macao Greater Bay Area (GBA Standard Contract), which aims to facilitate safe and orderly cross-boundary data flows within the Greater Bay Area, which includes 9 cities in China's Guangdong province and Hong Kong.[97] Alongside the release of the GBA Standard Contract, the PCPD also released guidance to help local organizations understand how the GBA Standard Contract: (1) applies to them, and (2) relates to the PCPD's existing RMCs.[98]

## International Cooperation

The PCPD actively shares experiences and contributes to data protection discourse through bilateral and multilateral engagements. In May 2023, the PCPD signed a Memorandum of Understanding (MoU) with the National Privacy Commission of the Philippines to strengthen ties and foster closer cooperation in personal data privacy protection.[99] The collaboration includes sharing information on investigations, providing mutual assistance in cross-border data incidents, and collaborating in training and education.

In July 2022, the PCPD renewed its 2019 MoU with Singapore's Personal Data Protection Commission, focusing on exchanging information and best practices on data protection policies and enforcement actions, as well as coordinating and providing mutual assistance in joint investigations into cross-border personal data incidents.

[92] https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_note_dbn_e.pdf
[93] https://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf
[94] https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn_form.html
[95] https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf
[96] https://www.pcpd.org.hk/english/news_events/media_statements/press_20220512.html
[97] http://www.cac.gov.cn/2023-12/13/c_1704042786237103.htm
[98] https://www.pcpd.org.hk/english/resources_centre/publications/files/standard_contract_gba.pdf
[99] https://www.pcpd.org.hk/english/news_events/media_statements/press_20230522.html

The PCPD actively participates in international forums such as the GPA, APPA Forum, Global Privacy Enforcement Network (GPEN), and the APEC Data Privacy Subgroup.[100]

[100] https://www.pcpd.org.hk/english/about_pcpd/external_connection/external_connection.html

# Japan

A review of the Personal Information Protection Commission (PPC)'s key strategic documents and recent regulatory actions reveals that its main priorities for 2024 include conducting a mandatory three-year review of the Act on the Protection of Personal Information (APPI) and promoting international cooperation, especially on cross-border data transfers. Over the last year and a half, the PPC has demonstrated a proactive approach to addressing challenges associated with emerging technologies like AI and biometrics, issuing guidance on generative AI and facial recognition technologies. Its enforcement actions have also focused on data breaches and security measures.

However, the PPC's role and approach may be subject to change in the near future, given the proposals put forward by the ruling Liberal Democratic Party. As Japan navigates the balance between data protection and innovation, the outcomes of the APPI review and potential structural changes to the PPC will be critical in shaping the country's data protection landscape in the coming years.

## Background

The primary data protection law in Japan is the APPI, which took effect in 2003 and underwent significant amendments in 2015, 2020, and 2021.

The PPC is Japan's primary regulatory authority for personal data protection. It was formally established in January 2016 and serves as an independent supervisory authority overseeing and enforcing the APPI, as well as the My Number Act, which governs the use of Japan's national identification number system. Following 2021 amendments to the APPI that took effect in March 2023, the PPC became responsible for supervising organizations in both the public and private sectors, as well as local governments.

The PPC is led by a chairperson and eight commissioners appointed by the Prime Minister with the consent of both houses of Japan's Parliament, the Diet.[101] The current chairperson is Shizuo Fujiwara, who assumed the role in January 2024.[102] The chairperson and commissioners serve five-year terms.

Key responsibilities of the PPC include:

- establishing and promoting basic policies for personal data protection;
- monitoring and supervising handling of personal data;
- certifying personal data protection organizations;
- resolving complaints regarding the handling of personal data;
- engaging in international cooperation; and

[101] https://www.ppc.go.jp/aboutus/mission-roles/
[102] https://www.ppc.go.jp/aboutus/mission-roles/iinchou_fujiwara/

- raising public awareness of personal data protection-related issues and issuing guidance.[103]

In line with its advisory function, the PPC also provides guidelines on various aspects of data protection, including general rules for handling personal information, offshore transfers, and requirements for providing personal information to third parties.[104] The PPC has also partnered with several sectoral regulators to issue guidelines on protection of personal data within specific sectors, including the healthcare, genetic testing, debt collection, employment, and financial sectors.[105]

The APPI grants the PPC broad powers to investigate potential breaches of the APPI, including the power to conduct on-site inspections.

The PPC generally addresses non-compliance with the APPI violations through a three-step enforcement mechanism. Initially, the PPC issues administrative guidance or a corrective recommendation to the organization to rectify the non-compliance. If the organization fails to comply without legitimate grounds and a serious infringement of data subjects' rights and interests is imminent, the PPC is empowered to issue a binding order. Non-compliance with this order is a criminal offense punishable by a fine of up to 100 million yen (approximately US$679,000). This approach reflects Japan's culture of prioritizing social reputation in data protection compliance.

## Overview of Key Strategic Documents

The PPC publishes several key strategic documents annually:

**Activity Policy** (個人情報保護委員会活動方針)
This document identifies the PPC's high-level direction for the year. In the 2024 edition, key priorities for the year[106] include: (1) legal reform by undertaking a mandatory three-year review of the APPI (see below); and (2) promoting cross-border data transfer mechanisms, in addition to continuing business-as-usual activities such as monitoring and supervision

**International Strategy** (個人情報保護委員会の国際戦略)
This document expands on the broad international goals identified in the Activity Policy. In the 2024 edition, key activities[107] include: (1) developing mutual recognition of data protection frameworks between Japan and jurisdictions whose data protection frameworks provide substantially equivalent protections to those under the APPI (abbreviated in this report as "adequacy" and distinct from adequacy under the GDPR regime); (2) promoting international certification systems; (3) introducing MCCs for global use; and (4) responding to risks to the protection of personal data.

[103] https://www.ppc.go.jp/aboutus/commission/; See also the PPC's Organizational Philosophy (2022), available at https://www.ppc.go.jp/files/pdf/soshikirinen_4.pdf
[104] https://www.ppc.go.jp/personalinfo/legal/#anc_Guide
[105] https://www.ppc.go.jp/personalinfo/legal/guidelines/
[106] https://www.ppc.go.jp/files/pdf/R6_katsudouhoushin.pdf
[107] https://www.ppc.go.jp/files/pdf/kokusai_senryaku_r6.pdf

**Monitoring and Supervision Policy** (個人情報保護委員会における監視 監督方針)
This policy outlines the PPC's approach to monitoring and supervising compliance with relevant laws and regulations. In the 2024 edition, key priorities[108] include: (1) promptly addressing data breach reports and conducting daily monitoring; (2) scheduling on-site inspections at approximately 50 to 60 institutions; and (3) conducting enforcement status surveys, with results to be compiled and made public later this year.

**Annual Report** (年次報 告)
Released in June 2024, the Annual Report provides an overview of the PPC's activities in the previous year and identifies the triannual review of the APPI, AI, and biometrics as key priorities during 2023.[109]

# Key Priorities

## Legal Reform

A major focus for the PPC in 2024 is conducting a mandatory three-year review of the APPI. This review, which was introduced through legal reforms to the APPI in 2020, is intended to ensure the APPI remains relevant in light of international trends, technological advancements, and new industries utilizing personal data.[110] The most recent review began in November 2023[111] and as of the date of this Report, remains ongoing.

In June 2024, the PPC published an **Interim Report on the Triannual Review of the APPI** (個人情報保護法 いわゆる3年ごと見直しに係る検討の中間整理, henceforth: Interim Report)[112] seeking feedback from stakeholders on several potential updates to the APPI, including:

- Establishing stricter rules for biometric data;
- Imposing stricter requirements for transferring personal data to third parties;
- Explicitly requiring parental consent for processing the personal data of minors under the age of 16;
- Enabling qualified consumer organizations to seek injunctions against illegal data practices;
- Implementing stricter penalties and a surcharge system for severe misuse of personal data; and
- Streamlining data breach reporting requirements.

On 4 September 2024, the PPC published a summary of stakeholder feedback received on the Interim Report.[113] According to the Interim Report, the PPC aims to finalize its recommendations by the end of 2024 based on this feedback.

However, it is important to note that a recent whitepaper by the ruling Liberal Democratic Party (LDP), titled "Digital Japan 2024," called for re-evaluation of the PPC's structure and practices to ensure that the agency promotes use of data to contribute to Japan's socio-economic progress. The paper, which was submitted to Prime Minister Fumio

[108] https://www.ppc.go.jp/files/pdf/kanshi_kantoku_06houshin.pdf
[109] https://www.ppc.go.jp/files/pdf/060611_annual_report.pdf
[110] https://www.ppc.go.jp/personalinfo/3nengotominaoshi/
[111] https://www.ppc.go.jp/files/pdf/231115_shiryou-2-1.pdf
[112] https://www.ppc.go.jp/news/press/2024/240627_02/
[113] https://www.ppc.go.jp/files/pdf/240904_shiryou-1-2.pdf

Kishida in May 2024, suggests potentially dividing the PPC's roles between different agencies. Notably, the proposal also recommends several areas for APPI reform, including:

- Reviewing definitions of "personal data" and related terms.
- Allowing provision of personal data to third parties without consent in certain cases.
- Facilitating use of pseudonymized data for statistical analysis.
- Expanding the timeframe for reviewing the APPI.
- Promoting cross-border data flows.

While it remains to be seen how the government will respond to these proposals, they could potentially lead to a more industry-friendly approach to data protection regulation in Japan if adopted.

## International Cooperation and Cross-Border Data Transfers

The PPC is actively engaged in international cooperation and is a participating member of the GPA, International Working Group on Data Protection in the Information and Communications Sector, G7 Data Protection and Privacy Authorities Roundtable, APPA Forum, Organization for Economic Cooperation and Development (OECD), and Asia-Pacific Economic Cooperation (APEC).[114]

It also actively engages with peer regulators in other jurisdictions. In 2023 and 2024, it met with representatives from the European Commission[115] and data protection authorities from Sri Lanka,[116] Malaysia,[117] and the United Kingdom (UK).[118] Notably, in October 2023, it also signed a memorandum of cooperation with the UK Information Commissioner's Office (ICO) that establishes a framework for information sharing in cross-border investigations.[119]

Based on the PPC's 2024 Activity Policy and International Strategy, key activities for 2024 include:

### (a) Promoting Cross-Border Data Transfers

Several of the PPC's strategic documents identify as a key priority for 2024 the promotion of "Data Free Flow with Trust" (DFFT) – a concept first raised at the G20 Osaka Summit in 2019 that aims to promote the free flow of data while ensuring trust in privacy, security, and intellectual property rights.[120] According to the PPC's 2024 Activity Policy, promoting DFFT entails establishing a safe and facilitative international environment for cross-border data transfers by:

- developing adequacy frameworks between Japan and other jurisdictions;

[114] https://www.ppc.go.jp/enforcement/cooperation/international_conference/
[115] https://www.ppc.go.jp/enforcement/cooperation/cooperation/240620_EU/; https://www.ppc.go.jp/enforcement/cooperation/20240304_EU/; https://www.ppc.go.jp/enforcement/cooperation/cooperation/230404_review/
[116] https://www.ppc.go.jp/enforcement/cooperation/20240514_SriLanka/
[117] https://www.ppc.go.jp/enforcement/cooperation/20240219_Malaysia/
[118] https://www.ppc.go.jp/enforcement/cooperation/cooperation/20231017_ico/; https://www.ppc.go.jp/enforcement/cooperation/cooperation/20230619_ico/
[119] https://www.ppc.go.jp/enforcement/cooperation/cooperation/ico_moc/
[120] https://www.digital.go.jp/en/dfft-en

- promoting international certification systems;
- introducing MCCs for global use; and
- responding to risks to the protection of personal data.

**Adequacy**

Article 28 of the APPI empowers the PPC to issue adequacy decisions which enable transfers of personal data from Japan to jurisdictions whose data protection frameworks provide substantially equivalent protections to those under the APPI. To date, the PPC has only issued adequacy decisions in favor of the European Union (EU) (January 2019) and the UK (March 2023).[121]

In April 2023, the PPC and the European Commission concluded the first review of their mutual adequacy decision.[122] The PPC's Activity Policy and International Strategy indicate that in 2024, the PPC aims to extend this mutual adequacy decision to the academic and public sectors. It also plans to initiate discussions with other likeminded jurisdictions on establishing mutual adequacy decisions.

**Promoting international certifications for cross-border data transfers**

The PPC's Activity Policy and International Strategy indicate that in 2024, the PPC will lead international discussions to develop the Global Cross-Border Privacy Rules (Global CBPRs) and promote participation by other jurisdictions in the Global CBPR Forum. It will also encourage adoption of Global CBPR certification by domestic businesses.

**Introducing global MCCs**

The PPC's Activity Policy and International Strategy indicate that in 2024, the PPC will work to introduce MCCs for global use. This initiative appears to be at an early stage, as the key activity for 2024 is **c**onducting joint research in fora like the G7 and GPA to promote interoperability between existing MCCs.

## (b) International Cooperation

Japan hosted the G7 countries in 2023, and in June of that year, the PPC convened the 3rd annual G7 Data Protection and Privacy Authorities Roundtable in Tokyo.[123] The PPC's Activity Policy and International Strategy indicate that in 2024, the PPC will leverage outcomes from the Roundtable at other international conferences. Notably in this regard, the PPC will be hosting the 62nd APPA Forum in November 2024.[124]

[121] https://www.ppc.go.jp/enforcement/cooperation/cooperation/sougoninshou/

[122] https://commission.europa.eu/news/joint-press-statement-conclusion-first-review-japan-eu-mutual-adequacy-arrangement-2023-04-04_en; https://www.ppc.go.jp/files/pdf/20230322_review_report.pdf

[123] https://www.ppc.go.jp/en/aboutus/roles/international/conference/g7rt_communique/

[124] https://www.appaforum.org/forums/

The PPC has also indicated that it plans to lead discussions on government access to data and data localization at the OECD, and pursue bilateral and regional cooperation, especially in the APAC region, including by signing memoranda of cooperation with likeminded jurisdictions in priority areas.

## AI

Addressing the data protection implications of generative AI emerged as a key priority for the PPC in 2023.
In June 2023, the PPC issued two guidance documents addressing the use of generative AI services under the APPI.

- The first, a "**Notice Regarding Cautionary Measures on the Use of Generative AI Services**" (生成 AI サービスの利用に関する注意喚起等), provides general guidance to businesses, administrative agencies, and general users. It emphasizes the principle of purpose limitation and advises businesses to provide personal data to generative AI services only when necessary for a specified purpose or with the data subject's consent.[125]
- The second, a "**Cautionary Notice to OpenAI**" (OpenAI に対する注意喚起の概要), outlines specific recommendations for OpenAI LLC, the developer of the generative AI service ChatGPT, to ensure ChatGPT's compliance with the APPI's requirements as to collection and use of sensitive personal data.[126]

The PPC's guidance, based on current data protection issues, may evolve with technological developments. Notably, in the Review Report on the PPC's triannual review of the APPI, the PPC indicated that it is considering measures to promote responsible use of personal data without consent for purposes like training generative AI systems.

## Biometrics

Regulating the use of facial recognition technology, particularly for crime prevention, is another key focus area for the PPC. Recent actions include:

- Releasing a report in March 2023 clarifying the application of Japanese data protection law to the use of facial recognition cameras for crime prevention and safety management.[127]
- Publishing guidance in March 2023 on complying with the APPI when using camera images for crime prevention and security purposes.[128]
- Updating the "**Q&A on Guidelines Regarding the Act on Personal Information Protection**" in May 2023 with 11 new provisions on the use of facial recognition cameras.[129]

These documents provide clarity on when data collected through facial recognition technologies qualifies as personal or sensitive personal data, when consent is required, and data subjects' rights regarding such data.

[125] https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf
[126] https://www.ppc.go.jp/files/pdf/230602_alert_AI_utilize.pdf
[127] https://www.ppc.go.jp/personalinfo/camerakentoukai/20230314/
[128] https://www.ppc.go.jp/files/pdf/kaoshikibetsu_camera_system.pdf
[129] https://www.ppc.go.jp/files/pdf/kaoshikibetsu_camera_system.pdf

## Children's Privacy

As highlighted in the Interim Report, enhancing protection for children's personal data has been identified as a priority in the PPC's review of the APPI. The review acknowledges the lack of specific provisions in the current APPI safeguarding children's personal information and explores potential amendments to address this gap. The review notes that the PPC has been drawing insights from comparable laws and regulations in jurisdictions like the EU, UK, and US to inform its approach.

## Enforcement

As discussed above, the PPC's enforcement approach typically involves issuing guidance and recommendations to bring organizations' data processing activities in compliance with the APPI, with binding orders imposed only as a last resort. According to its latest Annual Report, in 2023, the PPC issued guidance and advice in 333 cases and corrective recommendations in 3 cases, representing a threefold increase compared with the previous year.

Notable enforcement actions in 2023-2024 include:

- Issuing corrective recommendations to two subsidiaries of Nippon Telephone and Telegraph West following a data breach affecting over 9 million individuals.[130]
- Providing corrective guidance to MKSystems, an outsourced human resources services provider, after a ransomware attack compromised the personal data of approximately 7.5 million individuals.[131]
- Issuing a corrective order to LY Corporation, operator of Japan's largest messaging app LINE, in connection with two data breach incidents that compromised the personal data of approximately 520,000 individuals.[132]
- Conducting an on-site inspection and issuing administrative guidance to Japan's Digital Agency and National Tax Agency following a breach of the "My Number" national identity system.[133]

These enforcement actions highlight the PPC's focus on addressing inadequate security measures and improving incident response processes.

[130] https://www.ppc.go.jp/files/pdf/240124_houdou.pdf
[131] https://www.ppc.go.jp/news/press/2023/240325_houdou/
[132] https://www.ppc.go.jp/files/pdf/240328_houdou.pdf
[133] https://www.ppc.go.jp/news/press/2023/20230920_02/

# Malaysia

Over the last year, Malaysia's Personal Data Protection Department (PDPD) has been impacted by organizational changes and legal reforms to modernize the Personal Data Protection Act 2010 (PDPA), and international cooperation. The PDPD's priorities for 2024-2025 will likely focus on implementing forthcoming amendments to Malaysia's data protection framework that seek to modernize and align it with international standards. The upcoming changes, coupled with efforts in international cooperation, indicate that Malaysia is taking steps to enhance its data protection regime and position itself as a responsible player in the global digital economy.

However, the lack of publicly available information on the PCPD's enforcement actions and the absence of published strategy documents suggest there may be room for improvement in terms of regulatory clarity and public communication.

## Background

The PDPA is Malaysia's primary data protection legislation, which came into force on November 15, 2013. The PDPD, established in May 2011, is responsible for implementing and enforcing the PDPA.

The PDPD previously reported into the Ministry of Communications and Digital. However, in December 2023, the Malaysian Government established a new Digital Ministry as part of a cabinet reshuffle.[134] This ministry, led by a dedicated Digital Minister, now oversees the PDPD along with other digital economy-focused agencies[135] This reorganization signals the Malaysian Government's increased focus on digital transformation and data protection.

The PDPD is led by a Director General and Commissioner, currently Professor Dr. Mohd Nazri bin Kama[136] (who will serve until May 7, 2025). The Commissioner is advised by a Personal Data Protection Advisory Committee appointed by the Minister.[137]

The PDPD's mission is to regulate the processing of personal data in commercial transactions and protect data subjects from possible misuse of their data.[138] Key functions of the PDPD[139] include:

- Enforcing and regulating the PDPA;
- Managing a registration scheme for certain classes of data users;

[134] https://www.pmo.gov.my/2024/01/digital-ministry-formed-to-enable-country-to-compete-in-the-sector-pm-anwar/
[135] https://www.pdp.gov.my/jpdpv2/mengenai-kami/profil/pengenalan/
[136] https://www.pdp.gov.my/jpdpv2/mengenai-kami/profil/carta-organisasi/; https://www.pdp.gov.my/jpdpv2/berita_terkini/siaran-media-profesor-dr-mohd-nazri-bin-kama-ketua-pengarah-jabatan-perlindungan-data-peribadi-yang-baharu/
[137] https://www.pdp.gov.my/jpdpv2/mengenai-kami/maklumat-organisasi/jawatankuasa-penasihat/
[138] https://www.pdp.gov.my/jpdpv2/mengenai-kami/profil/objektif/
[139] https://www.pdp.gov.my/jpdpv2/mengenai-kami/profil/fungsi-peranan/

- Approving and registering codes of practice for specific sectors; and
- Conducting investigations and enforcing compliance.

The Commissioner has broad enforcement powers, including the ability to search and seize, access computerized data, require production of documents, examine persons related to cases, and make arrests without warrants for offenses under the PDPA.

Part II, Division 2 of the PDPA also assigns the Commission a key role in managing the PDPA's registration scheme for data users (i.e., controllers). This scheme requires data users who fall within in 13 classes prescribed by the Personal Data Protection (Class of Data Users) Order 2013[140] (as amended in 2016)[141] to apply for registration with the PDPD. Generally, these include data users who are subject to sectoral regulation, including those in the healthcare, banking and finance, insurance, education, and aviation sectors. Processing personal data without a valid certificate is an offense under the PDPA punishable by fines and/or imprisonment. In May 2024, the PDPD published an updated circular outlining the costs and procedure for registration.[142]

Part II, Division 3 of the PDPA empowers the Commissioner to designate a body, known as "data user forum," to represent a prescribed class of data users and register codes of practice developed by such bodies. These codes set out more detailed requirements than those in the PDPA for processing personal data, taking into account the industry practices of the specific sector. Once a code has been registered, all data users within the prescribed data user forum must comply with the provisions of the code. To date, the Commissioner has approved and registered seven such codes.[143] The PDPD also released a general code of practice in December 2022 that applies to registered data users not covered by sector-specific codes.[144]

## Overview of Key Strategic Documents

The PDPD does not publish comprehensive strategy documents. However, it previously released annual reports from 2014 to 2021, which outlined the department's purpose, mission, and key activities.[145]

[140] https://lom.agc.gov.my/act-view.php?type=pua&no=P.U.%20(A)%20336/2013
[141] https://lom.agc.gov.my/act-view.php?type=pua&no=P.U.%20(A)%20326/2016
[142] https://www.pdp.gov.my/jpdpv2/pengumuman/pekeliling-pesuruhjaya-perlindungan-data-peribadi-bil-1-2024-kewajipan-pendaftaran-dan-pembaharuan-perakuan-pendaftaran-sebaga-pengguna-data-di-bawah-akta-perlindungan-data-peribadi-2010-akta-709/
[143] https://www.pdp.gov.my/jpdpv2/assets/2019/09/Code_of_Practice_Insurance_and_Takaful_2016.r1.pdf; https://www.pdp.gov.my/jpdpv2/assets/2019/09/170816-ABM-Code-Of-Practice-CLOcv04-FINAL_CLEAN.pdf; https://www.pdp.gov.my/jpdpv2/assets/2019/09/Code_of_Practice_For_Aviation_Sector.pdf; https://www.pdp.gov.my/jpdpv2/assets/2019/09/Communications-Sector-PDPA-COP-1.pdf; https://www.pdp.gov.my/jpdpv2/assets/2019/09/COP-English-JUNE-2016-13072016-amendment-clean-copy-toJPDM.pdf; https://www.pdp.gov.my/jpdpv2/assets/2022/02/COP_CODE-OF-PRACTICE-Personal-Data-Protection-Water.pdf
[144] https://www.pdp.gov.my/jpdpv2/assets/2023/01/28.12.2022-FINAL-PRINTING-COP-BI.pdf
[145] https://www.pdp.gov.my/jpdpv2/laporan_tahunan

# Key Priorities

## Legal Reform

The Malaysian Government has been working on significant amendments to the PDPA since 2020. After an initial public consultation in February 2020,[146] progress stalled due to the COVID-19 pandemic and political factors. However, the process regained momentum following the election of a new Federal Government in November 2022 and the subsequent establishment of the Digital Ministry (see above).

On July 10, 2024, Digital minister Gobind Singh Deo tabled a bill to amend the PDPA[147] in Parliament. It was passed by the House of Representatives on July 16, 2024 and by the Senate on July 31, 2024. The bill is presently awaiting Royal Assent and will come into effect on a date to be appointed by the Digital Minister.

Key provisions of the amendment bill include:

- Mandatory appointment of Data Protection Officers (DPOs) by data controllers and processors.
- Mandatory data breach notification to the Commissioner, with fines of up to MYR 250,000 (approximately US$53,130) and/or imprisonment for up to two years for non-compliance with data breach notification requirements.
- Introduction of data subjects' right to data portability.
- Extension of security obligations to data processors.
- Revised rules for international data transfers, allowing transfers to jurisdictions with substantially similar laws or adequate levels of protection

The bill also increases the maximum penalty for breaching PDPA principles from MYR 300,000 (approximately US$67,500) to MYR 1 million (approximately US$212,500). Potential imprisonment terms have also been increased from two to three years.

## Enforcement

While the PDPD has broad enforcement powers, it does not publish a formal enforcement policy. Information about enforcement actions is also limited. Typically, the PDPC only publishes a summary of compound offenses and prosecutions on its website.[148]

The latest summary, published in end-July 2024, indicates that the 90% penalties imposed by the PDPD to date in 2024 have been for failure to register or renew a registration under Part II, Division 2 of the PDPA. In all cases, fines were imposed, with the quantum ranging from MYR 13,750 (approximately US$3,100) to MYR 50,000 (approximately US$11,300).[149]

[146] https://www.pdp.gov.my/jpdpv2/assets/2020/02/Public-Consultation-Paper-on-Review-of-Act-709_V4.pdf
[147] https://www.parlimen.gov.my/files/billindex/pdf/2024/DR/DR%2021%20BM.pdf
[148] https://www.pdp.gov.my/jpdpv2/awam/senarai-kompaun/
[149] https://www.pdp.gov.my/jpdpv2/awam/senarai-kompaun/

## International Cooperation

The PDPD is a member of the APPA Forum[150] and has been actively engaging in international cooperation efforts:

- In January 2023, Malaysia signed a memorandum of understanding with Singapore to cooperate in personal data protection, cybersecurity, and digital economy matters.[151]
- On June 11, 2024, the PDPD published a memorandum of cooperation signed with Türkiye's Personal Data Protection Authority (KVKK) for mutual assistance in privacy and personal data protection.[152]

[150] https://www.appaforum.org/members/

[151] https://www.channelnewsasia.com/singapore/digital-green-economy-agreement-singapore-malaysia-anwar-visit-3240741

[152] https://www.pdp.gov.my/jpdpv2/pengumuman/memorandum-kerjasama-pejabat-pesuruhjaya-pdp-dengan-kvkk-turkiye-tingkat-keupayaan-rentas-negara/

# New Zealand

Based on its key strategic documents and recent actions, the Office of the Privacy Commissioner (OPC) of New Zealand's top priorities for 2024-2025 are: (1) strengthening compliance and enforcement functions, (2) delivering on regulatory stewardship responsibilities, and (3) ensuring the Privacy Act 2020 remains fit for purpose in the digital age. The OPC is actively working on initiatives related to biometrics, children's privacy, legal reforms to address modern challenges like AI and data breaches, and international cooperation. Key focus areas include developing a biometrics privacy code, assessing privacy safeguards for children and young people, advocating for updates to the Privacy Act, and providing guidance on AI compliance.

## Background

The Privacy Act 2020 provides the primary rules for processing personal information in New Zealand, articulated through 13 Information Privacy Principles (IPPs).[153]

The OPC[154] serves as the main regulator for administering and enforcing the Privacy Act. The OPC was first established in 1993 under the now-repealed Privacy Commissioner Act 1991. Presently, it is recognized as an independent crown entity under the Crown Entities Act 2004.[155] This means that it is funded by the state, but operates independently from government policy or ministerial control.[156]

The OPC has a wide range of functions, which are listed in Section 17 of the Privacy Act. Key functions include:

- Investigating and taking enforcement action in relation to breaches of the Privacy Act;
- Developing codes of practice for specific industries or sectors;
- Monitoring inquiring into matters that may affect individual privacy;
- Education and awareness;
- Examining draft legislation for its possible impact on individual privacy; and
- Reporting to the New Zealand government on matters affecting privacy, both domestic and international.

The OPC's leadership comprises the Privacy Commissioner, Deputy Privacy Commissioner, General Manager, Assistant Commissioner for Strategy, Policy and Engagement, and General Counsel.[157] The current Privacy Commissioner is Michael Webster (since July 2022).

[153] https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html
[154] OPC official website https://www.privacy.org.nz/
[155] https://www.legislation.govt.nz/act/public/2004/0115/latest/DLM329631.html
[156] https://www.privacy.org.nz/about-us/what-we-do/
[157] https://www.privacy.org.nz/about-us/who-we-are/

As stated above, a key function of the OPC is issuing codes of practice that modify the application of IPPs for specific industries, organizations, or types of information. To date, the OPC has issued six codes of practice, including codes for the health, telecommunications, and credit reporting sectors.[158]

The OPC's active enforcement actions are selective and often driven by specific circumstances. The Privacy Act's enforcement mechanism primarily relies on individuals lodging complaints when they become aware of potential privacy breaches. However, the Privacy Commissioner retains the authority to initiate investigations into any matter where there are concerns about potential privacy infringements, even without a formal complaint.

The OPC publishes its compliance and regulatory action policy[159] and complaint handling policy.[160] The OPC generally seeks to resolve complaints through conciliation and mediation. If a settlement cannot be reached, the Privacy Commissioner may conduct a formal investigation and issue an opinion, which is highly persuasive though not legally binding. The Privacy Commissioner can also issue compliance notices[161] for breaches, which if not followed, can lead to enforcement proceedings with potential fines of up to NZ$10,000 (approximately US$6,200). In 2021, the OPC issued its first compliance notice to the Reserve Bank of New Zealand, in response to a cyberattack in December 2020.[162]

The Privacy Commissioner also has a "name and shame" policy to publicly identify agencies that have breached the Privacy Act in certain circumstances.

The Privacy Act does not allow for punitive fines to be imposed directly for privacy breaches. Instead, the Privacy Act empowers the Human Rights Review Tribunal – a judicial body which deals with cases dealing with New Zealand's main pieces of human rights law (including the Privacy Act) – to order agencies that have interfered with an individual's privacy to pay compensation to affected individuals. However, the individual must establish harm to qualify for damages.

## Overview of Key Strategic Documents

The OPC's strategic priorities are outlined in several key documents:

**Statement of Intent 2023-2027**[163]

[158] https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/

[159] https://www.privacy.org.nz/about-us/what-we-do/caraf/

[160] https://www.privacy.org.nz/assets/New-order/About-us/Transparency-and-accountability-/Complaint-Handling-Policy-v2.pdf

[161] See https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Statements-and-media-releases/2.-Compliance-Notice-Guidelines.pdf

[162] https://www.privacy.org.nz/publications/statements-media-releases/privacy-commissioner-issues-first-compliance-notice-to-reserve-bank-of-new-zealand/

[163] https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Corporate-reports/Statement-of-Intent-OPC-1-July-2023-to-30-June-2027.pdf

Published in June 2023, this document sets out the OPC's medium-term intentions over a five-year period. It identifies four high-level objectives:

- Partnering with Māori on privacy.
- Engaging and empowering vulnerable communities.
- Setting clear expectations for agencies.
- Using full powers to hold agencies accountable for serious privacy harms.

**Statement of Performance Expectations 2024-2025 (SPE)**[164]

Released annually, this document aligns with the Statement of Intent but focuses on immediate strategic priorities for the coming year. The latest SPE, published in July 2024, identifies three key priorities:

- Strengthening compliance and enforcement functions.
- Delivering on regulatory stewardship responsibilities.
- Ensuring the Privacy Act remains fit for purpose in the digital age.

**Annual Report of the OPC for 2023**

The OPC publishes annual reports outlining its progress towards achieving its strategic objectives, activities, and financial performance report. The latest, published in November 2023, covers the period of July 2022 to June 2023.[165]

In addition, the OPC also uses various other documents to communicate its vision and ensure transparency, including quarterly reports to the Minister of Justice,[166] guidance documents,[167] insight reports,[168] speeches and presentations,[169] and submissions to government consultations.[170]

# Key Priorities

## Biometrics

The OPC has been actively developing a biometrics privacy code since November 2023.[171] In April 2024, the OPC released an exposure draft of the code,[172] proposing new rules for agencies involved in the collection or use of biometric data. Key provisions include:

- Proportionality assessments for collecting biometric information.

---

164 https://privacy.org.nz/assets/New-order/Resources-/Publications/Corporate-reports/Statement-of-Performance-Expectations-OPC-FINAL-June-2024-A985682.pdf

165 https://www.privacy.org.nz/publications/corporate-reports/annual-report-of-the-privacy-commissioner-2023/

166 https://www.privacy.org.nz/publications/corporate-reports/quarterly-reports-to-the-minister-of-justice/

167 https://www.privacy.org.nz/publications/guidance-resources/

168 https://www.privacy.org.nz/publications/insights-reports/

169 https://www.privacy.org.nz/publications/speeches-and-presentations/

170 https://www.privacy.org.nz/publications/reports-to-parliament-and-government/

171 https://privacy.org.nz/publications/statements-media-releases/privacy-commissioner-to-consult-on-new-rules-for-biometrics/

172 https://www.privacy.org.nz/assets/New-order/News/Consultations/Biometrics-April-2024/2024-04-10-Exposure-draft-of-Biometrics-Code.docx

- Enhanced transparency and notification obligations concerning the organization's collection and use of biometric data.
- Restrictions on using biometric information to infer health status or emotion or to categorize individuals.

The draft code also provides new definitions for key terms as well as exceptions for law enforcement, serious threats, and publicly available information.

In August 2024, the OPC published a report summarizing 250 submissions received during the public consultation.[173] The feedback highlighted significant public concern over biometric technologies, particularly regarding surveillance and commercial exploitation. The OPC is now considering this feedback to refine the proposals and develop draft guidance. The OPC is expected to reach a decision on whether to proceed with the code later in 2024.

In a related development, on April 4, 2024, the OPC announced an inquiry into a six-month trial of facial recognition technology by a major national supermarket chain, Foodstuffs North Island (FSNI).[174] This inquiry aims to ensure FSNI's compliance with the Privacy Act and assess the effectiveness of facial recognition technology in reducing harmful behavior in stores.

## Children's Privacy

Enhancing the protection of children's privacy is another priority area for the OPC. In September 2023, the OPC launched the Children and Young People's Privacy project to assess the adequacy of current privacy safeguards for children and young people.[175]

In April 2024, the OPC published a report summarizing 113 stakeholder responses received during a public consultation held from August to November 2023.[176] The report identified three key themes:

1. Need for guidance to help children and professionals understand existing privacy rules.
2. Requirement for regulatory changes to improve children's privacy protection.
3. Significant concerns around children's use of social media and associated privacy risks.

The OPC indicated it will continue to explore these issues and potential solutions, with plans to finalize its approach in the coming months.

[173] https://www.privacy.org.nz/assets/New-order/News/070824-Summary-of-submissions-FINAL-A998874.pdf
[174] https://www.privacy.org.nz/publications/statements-media-releases/inquiry-into-foodstuffs-north-islands-frt-trial-starts-today/
[175] https://www.privacy.org.nz/news/consultations/children-and-young-peoples-privacy-project-page/
[176] https://www.privacy.org.nz/assets/New-order/News/Consultations/Children-and-Young-Peoples-Privacy-pollicy-project/CYP-April-2024-release/Safeguarding-childrens-privacy-in-NZ-full-report.pdf

## Legal Reforms

The OPC is advocating for updates to the Privacy Act to address modern challenges like data breaches, AI, and facial recognition. The Annual Report emphasizes the need for a fit-for-purpose privacy law capable of addressing challenges posed by the digital age.

However, it is important to note that while the OPC can make recommendations to the New Zealand Government, it does not have the power to shape policy or propose draft amendments to the Privacy Act. Rather, the Ministry of Justice oversees the Privacy Act and any potential changes.

Most recently, In March 2024, the Privacy Commissioner publicly called for amendments to the Privacy Act during a speech at the National Cyber Security Summit in Wellington.[177] Specific proposals for amendment included:

- Introducing civil penalties for major non-compliance, highlighting the disparity in maximum fines provided for in the respective Privacy Acts of New Zealand (NZ$10,000, or approximately US$6,200) and Australia (A$50 million, or approximately US$33.7 million).
- Creating new privacy rights for New Zealanders.
- Strengthening requirements around automated decision-making.
- Imposing greater transparency obligations for agencies.

## AI

The OPC has been actively engaging with AI-related privacy issues:

- **Generative AI Guidance**: In June 2023, the OPC issued guidelines on its expectations regarding the use of generative AI, outlining eight points of advice for New Zealand agencies, businesses, and organizations to comply with the Privacy Act when engaging with generative AI.[178] Key recommendations include seeking senior leadership approval, conducting privacy impact assessments, and ensuring transparency about the use of generative AI.
- **AI and IPPs Guidance**: On September 21, 2023, the OPC published guidelines on complying with the 13 IPPs when using AI systems.[179] These guidelines build on the earlier statement on generative AI and provide detailed recommendations on various aspects of AI use, including privacy impact assessments, data collection, security, automated decision-making, and cross-border data transfers.

The OPC is also a member of the Global Privacy Assembly's International Enforcement Cooperation Working Group (IEWG) and signed its joint statement on data scraping and the protection of privacy in August 2023.[180]

---

177 https://www.privacy.org.nz/publications/statements-media-releases/greater-penalties-needed-privacy-commissioner-speaks-to-national-cyber-security-summit/

178 https://www.privacy.org.nz/publications/guidance-resources/ai/generative-artificial-intelligence/

179 https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/AI-Guidance-Resources-/AI-and-the-Information-Privacy-Principles.pdf

180 https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf

## International Cooperation

The OPC maintains an international engagement strategy, although the latest version only covers the period of 2018 to 2021 and has not been updated since then.[181]

Recent international cooperation efforts include:

- On January 15, 2024, the European Commission reaffirmed New Zealand's adequacy status following a review of 11 existing adequacy decisions.[182] On January 23, 2024, Privacy Commissioner Michael Webster issued a press release highlighting the significance of New Zealand maintaining EU adequacy status, and emphasizing the status' positive impact on trade and facilitating cross-border data transfers.[183]
- In August 2023, the OPC signed a Memorandum of Understanding on information sharing with Australia's privacy authority, the OAIC.[184]

The OPC is also a member of the APPA Forum.[185]

181 https://www.privacy.org.nz/assets/zLEGACY-FILES/Policies-and-values-transparency/international-engagement-strategy-2018-2021.docx

182 https://ec.europa.eu/commission/presscorner/detail/en/ip_24_161

183 https://www.privacy.org.nz/publications/statements-media-releases/new-zealand-is-adequate-and-we-couldnt-be-happier-about-itnew-news-page/

184 https://www.privacy.org.nz/assets/New-order/About-us/Transparency-and-accountability-/2023-08-18-FINAL-Information-Sharing-MOU-Between-the-OPC-and-the-OAIC-Signed-by-Liz-and-Libby-A889432.pdf

185 https://www.appaforum.org/members/

# The Philippines

Based on its recent actions, the National Privacy Commission (NPC) of the Philippines appears to prioritize ensuring organizations protect personal data from unauthorized access. The NPC has proactively issued guidance and educated stakeholders on Philippine data protection law. Key focus areas include legitimate interests, consent, deceptive design, identification cards, and a data competency program. The NPC actively participates in international forums and engages proactively with other data protection authorities.

## Background

The Data Privacy Act of 2012 (DPA), effective September 8, 2012, governs data privacy in the Philippines.[186] The DPA's Implementing Rules and Regulations (IRR) took effect on September 9, 2016.[187]

The NPC[188] is an independent statutory body responsible for administering, implementing and enforcing the DPA. Established in 2016 under Section 7 of the DPA, the NPC is attached to the Department of Information and Communications Technology. The NPC is currently headed by Commissioner John Henry D. Naga.[189]

The NPC's responsibilities include rulemaking, advising on personal data protection, public education, monitoring compliance, investigating and adjudicating complaints, and enforcing the DPA.

## Overview of Key Strategic Documents

The NPC does not publish a comprehensive strategy document. It does periodically publish annual reports:[190] the latest, covering 2022, was released in August 2023.[191] However, no report has been published for 2023 to date. The NPC also regularly updates its website with circulars and advisories,[192] advisory opinions,[193] and press releases.[194]

## Key Priorities

The following is a summary of priority areas for the NPC based on key regulatory actions in 2023 and 2024.

[186] https://privacy.gov.ph/data-privacy-act/
[187] https://privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/
[188] https://privacy.gov.ph/
[189] https://privacy.gov.ph/about-us/#organizational
[190] https://privacy.gov.ph/annual-reports/
[191] https://privacy.gov.ph/wp-content/uploads/2023/08/NPC-2022-ANNUAL-REPORT_ver3_revised.pdf
[192] https://privacy.gov.ph/pips-and-pics/advisories-circulars/
[193] https://privacy.gov.ph/pips-and-pics/advisory-opinions/
[194] https://privacy.gov.ph/news-2/

## Enforcement

Enforcement appears to be a key NPC priority and is expected to increase throughout 2024. Notably, in January 2024, the NPC amended its Rules of Procedure to streamline enforcement and enhance its investigatory powers, including introducing various new forms of "compliance checks."[195] These include:

- permitting the NPC to conduct spot checks in public areas where personal data is processed;
- reducing the notice period for on-site inspections by the NPC from 10 to 5 days; and
- allowing the NPC to conduct on-site inspections without notice where there are "persistent issues" or "substantial findings" of non-compliance with the DPA or other NPC issuances.

Since the amendments, the NPC has actively used its new powers, such as on-the-spot check of various retailers at one of the largest malls in the Philippines to assess their compliance with Philippine privacy law.[196] We expect that the NPC will continue to make use of these new powers to conduct on-site investigations throughout 2024.

## Rulemaking and Advisory

The NPC has proactively issued guidance to educate stakeholders on their obligations under the DPA. Between November and December 2023, the NPC released guidelines on:

- relying on consent[197] and legitimate interests[198] as legal bases to process personal data under the DPA;
- deceptive design;[199]
- issuing physical or digital identity cards;[200] and
- comprehensive operational measures to secure personal data.[201]

## Ecosystem Building

In 2023 and 2024, the NPC has introduced several registration, accreditation, and certification programs to strengthen data privacy and protection in the Philippines.

- **Data Competency Program**: NPC Circular 2023-02 established the Data Privacy Competency Program to improve data privacy education.[202] It empowers the NPC to license qualified training providers to design courses based on an NPC-specified curriculum.

---

195 https://privacy.gov.ph/wp-content/uploads/2024/01/NPC-Circular-2024-01-Amendments-to-the-2021-Rules-of-Procedure-of-the-NPC-FOR-PUBLICATION.pdf

196 https://privacy.gov.ph/privacy-commissioner-naga-warns-establishments-that-non-compliance-with-dpa-may-result-in-fines/

197 https://privacy.gov.ph/wp-content/uploads/2023/11/NPC-Circular-No.-2023-04_Guidelines-on-Consent_07Nov2023.pdf

198 https://privacy.gov.ph/wp-content/uploads/2024/03/NPC-Circular-Repeal-16-01-Signed.pdf

199 https://privacy.gov.ph/wp-content/uploads/2023/11/NPC-Advisory-No.-2023-01-Guidelines-on-Deceptive-Design-Patterns_7Nov23.pdf

200 https://privacy.gov.ph/wp-content/uploads/2023/11/Published-NPC-Circular-No.-2023-03_Guidelines-on-Identification-Cards_07Nov2023.pdf

201 https://privacy.gov.ph/wp-content/uploads/2024/03/NPC-Circular-Repeal-16-01-Signed.pdf

202 https://privacy.gov.ph/wp-content/uploads/2023/11/Circular-on-Data-Privacy-Competency-Program-2023.09.26.pdf

- **NPC Registration System**: In December 2022, the NPC established a mandatory registration framework for controllers and processors.[203] The framework requires entities to register if they employ over 250 people, process the sensitive data of over 1,000 individuals, or handle personal data that may pose a risk to data subjects' rights and freedoms. The framework became effective on January 11, 2023.
- **Philippine Privacy Mark Certification Program**: In October 2023, the NPC issued a circular outlining prerequisites for voluntary Philippine Privacy Mark certification and outlining requirements for accreditation of certification bodies.[204]

## Cybersecurity

As with many other jurisdictions internationally, a rise in cyberattacks in 2023 and 2024 has made responding to cybersecurity incidents a priority for the NPC. Mandatory data breach notification requirements are found in the IRR and NPC Circular 16-03, issued in December 2016.[205] In April 2022, the NPC established a formal Data Breach Notification Management System to receive data breach notifications and security reports.[206]

Throughout 2023 and 2024, the NPC's Complaints and Investigation Division responded proactively to several major security incidents, including those affecting the Philippines National Police (April 2023),[207] mobile payments application GCash (May 2023),[208] the Philippine Health Insurance Corporation (September 2023)[209] and the Philippines' Department of Science and Technology (April 2024).[210]

## International Cooperation

The NPC actively participates in international forums and engages bilaterally with other data protection authorities. Throughout 2023, the NPC signed Memoranda of Understanding with DPAs in Canada,[211] Malta,[212] Dubai International Finance Centre,[213] and Hong Kong.[214]

---

[203] https://privacy.gov.ph/npc-launches-online-registration-system-for-data-processing-systems/

[204] https://privacy.gov.ph/wp-content/uploads/2024/03/Prerequisites-for-the-Philippine-Privacy-Mark-Signed.pdf

[205] https://privacy.gov.ph/npc-circular-16-03-personal-data-breach-management

[206] https://privacy.gov.ph/npc-launches-user-friendly-online-system-for-faster-and-easier-data-breach-notification-management-and-reporting/

[207] https://privacy.gov.ph/npc-to-meet-with-law-enforcement-agencies-over-alleged-breach-of-personal-data/; https://privacy.gov.ph/statement-of-privacy-commissioner-john-henry-naga-on-the-alleged-leak-of-personal-data-among-law-enforcement-agencies/

[208] https://privacy.gov.ph/npc-concludes-investigation-on-unauthorized-gcash-transactions/

[209] https://privacy.gov.ph/press-statement-on-alleged-philhealth-data-breach/

[210] https://privacy.gov.ph/press-statement-of-the-npc-on-alleged-dost-data-breach/

[211] https://privacy.gov.ph/npc-strengthens-global-data-protection-cooperation-with-canada-and-malta/

[212] https://privacy.gov.ph/npc-strengthens-global-data-protection-cooperation-with-canada-and-malta/

[213] https://privacy.gov.ph/npc-and-difc-gains-stronger-foothold-through-mou-signing/

[214] https://privacy.gov.ph/ph-hk-sign-mou-on-personal-data-protection/

The NPC promotes cross-border data flow cooperation through its Global CBPR Forum participation. In March 2024, it joined the Global Cooperation Arrangement for Privacy Enforcement (CAPE) to enhance collaboration on cross-border data protection and privacy enforcement.[215] The NPC is also a member of the APPA Forum.[216]

[215] https://privacy.gov.ph/ph-promotes-global-cooperation-on-cross-border-data-protection-and-privacy-enforcement/
[216] https://www.appaforum.org/members/

# Singapore

Based on enforcement actions in 2023-24, the Personal Data Protection Commission (PDPC)'s top priority is ensuring organizations protect personal data from unauthorized access, imposing financial penalties in most cases. The PDPC is also actively encouraging responsible AI development, releasing a proposed AI governance framework for generative AI. Children's privacy is another key focus, with the PDPC issuing guidelines on processing children's data and exploring privacy-preserving age estimation. The PDPC continues to support privacy-enhancing technologies through its PET Sandbox and industry collaboration. While not yet in force, the PDPC is laying the groundwork for data portability rights. The PDPC also prioritizes international cooperation on data protection issues.

## Background

Singapore's primary legislation governing personal data protection, the Personal Data Protection Act (PDPA), was enacted on October 15, 2012.[217] The PDPA establishes a baseline standard for personal data protection in Singapore, addressing aspects such as consent, notification, purpose, access, correction, portability, security, data breach notification, accuracy, retention, and overseas transfers. It also establishes a national "Do Not Call Registry" allowing individuals to opt out of unwanted telemarketing messages.

The PDPC was established on January 2, 2013, to administer and enforce the PDPA. This role later passed to the Infocomm Media Development Authority (IMDA) in 2016,[218] with the PDPC's decision-making powers delegated to a Commissioner for Personal Data Protection. The current Commissioner is Lew Chuen Hong (since 2020)[219] and the Deputy Commissioner is Denise Wong (since 2023).[220]

The PDPC's stated aim is "to balance the protection of individuals' personal data with organizations' need to use the data for legitimate purposes."[221] To achieve this, the PDPC implements policies relating to personal data protection and develops advisory guidelines to help organizations understand and comply with the PDPA. The PDPC is structured to ensure this balance: within the IMDA organizational structure, the PDPC is in fact known as the Data Innovation and Protection Group.

Under the PDPA, the PDPC is empowered to take enforcement actions for contraventions of data protection requirements.

[217] https://sso.agc.gov.sg/Act/PDPA2012
[218] https://www.imda.gov.sg/regulations-and-licences/regulations/acts-and-regulations
[219] https://www.pdpc.gov.sg/news-and-events/announcements/2020/06/new-commissioner-for-personal-data-protection-commission
[220] https://www.pdpc.gov.sg/who-we-are/about-us
[221] https://www.pdpc.gov.sg/who-we-are/about-us

A common enforcement mechanism is imposition of financial penalties. Following amendments in October 2022, the maximum financial penalty under the PDPA increased to the higher of 10% of the organization's annual turnover in Singapore or S$1,000,000 (approximately US$750,000). The quantum of the penalty varies based on factors such as the breach's scale, remedial actions taken, and the organization's cooperation with the PDPC.

As of the date of this report, the largest fines issued by the PDPC were against two health-tech companies, Integrated Health Information Systems (S$750,000, approximately US$577,500) and Singapore Health Services (S$250,000, approximately US$192,500) for failing to make reasonable security arrangements to protect individuals' personal data.[222] The fines were issued following a major cyberattack in 2019 that compromised millions of individuals' personal data, including medical records.

Another common enforcement mechanism is to issue binding directions to infringing organizations, such as:

- Stopping the collection, use, or disclosure of personal data in contravention of the PDPA;
- Destroying personal data collected in contravention of the PDPA; and
- Providing or refusing access to or correction of personal data.

These directions may be registered with the courts and have the force and effect of a court order.

The PDPC can also accept undertakings from organizations voluntarily committing to implement remediation plans and resolve data breaches upon early detection.

The PDPC publishes detailed guidance on how it exercises its enforcement powers under the PDPA in its **"Advisory Guidelines on Enforcement Data Protection Provisions**," which were released in April 2016 and last updated in October 2022.[223]

## Overview of Key Strategic Documents

The PDPC does not publish a comprehensive strategy document. However, it actively updates its website with press releases and enforcement decisions. The PDPC also publishes an annual digest covering the year's decisions and articles contributed by the data protection legal community. The latest digest, covering 2022, was published in July 2023.[224]

## Key Priorities

The following is a summary of priority areas for the PDPC and IMDA based on key regulatory actions in 2023 and 2024.

[222] https://www.pdpc.gov.sg/all-commissions-decisions/2019/01/breach-of-the-protection-obligation-by-singhealth-and-ihis
[223] https://www.pdpc.gov.sg/guidelines-and-consultation/2020/02/advisory-guidelines-on-enforcement-of-data-protection-provisions
[224] https://www.pdpc.gov.sg/news-and-events/announcements/2023/07/pdp-digest-2022-now-available

## Enforcement and Data Breaches

The PDPC is active in enforcing the PDPA and generally focuses on raising data protection standards across domestic companies, especially small and medium-sized enterprises.

As of the date of this Report, the PDPC has issued a total of nine decisions in 2024. The majority of these decisions pertained to organizations' obligation to protect personal data from unauthorized access. In seven out of the nine cases, the PDPC imposed financial penalties ranging from S$9,000 (approximately US$6,900) to S$74,000 (approximately US$57,000). The second most common enforcement action was the issuance of directions, which occurred in approximately one-third of the cases.

In the previous year, 2023, the PDPC issued a total of 17 enforcement decisions. Similar to the trend observed in 2024, the majority of these cases (12 out of 17) dealt with the requirement for organizations to safeguard personal data against unauthorized access. Financial penalties were imposed in nine out of the 17 cases, with the quantum of the fines ranging from S$8,000 (approximately US$6,200) to S$82,000 (approximately US$63,100). Directions were issued by the PDPC in seven out of the 17 cases.

Based on the enforcement actions taken by the PDPC in 2023 and the first few months of 2024, it is evident that the PDPC places a strong emphasis on ensuring that organizations fulfill their obligation to protect personal data from unauthorized access. The PDPC has consistently utilized financial penalties and the issuance of directions as the primary tools to enforce compliance with data protection regulations in Singapore.

## AI

AI has long been a key priority for the PDPC and IMDA, which in previous years, have taken a forward-thinking approach to AI governance by creating the world's first "**Model AI Governance Framework"** (now in its second edition)[225] and a governance testing and framework and toolkit known as AI Verify.[226]

AI has continued to be a key priority 2023 and 2024. Notably, in June 2023, the IMDA launched the AI Verify Foundation to advance responsible AI use through open-source testing tools and best practices.[227] Together with the AI Verify Foundation, the IMDA has been working to develop responsible AI governance frameworks and tools.

- In June 2023, the IMDA and the AI Verify Foundation and open-sourced AI Verify.[228]

[225] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf

[226] https://www.pdpc.gov.sg/news-and-events/announcements/2022/05/launch-of-ai-verify---an-ai-governance-testing-framework-and-toolkit

[227] https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/singapore-launches-ai-verify-foundation

[228] https://www.imda.gov.sg/-/media/imda/files/news-and-events/media-room/media-releases/2023/06/7-jun---ai-annoucements---annex-a.pdf

- In October 2023, the IMDA and the US National Institute of Standards and Technology (NIST) released a joint "crosswalk" guide mapping the requirements of AI Verify to those of NIST's AI Risk Management Framework.[229]

The IMDA's focus on AI also expanded to generative AI in 2023 and 2024. In June 2023, the IMDA and the AI Verify Foundation released a discussion paper on the implications of generative AI for trust and governance,[230] identifying risks in six key areas: (1) accountability; (2) data; (3) model development and deployment; (4) assurance and evaluation; (5) safety and alignment research; and (6) "Generative AI for Public Good."

Based on feedback from the discussion paper, the IMDA and the AI Verify Foundation released a "**Proposed Model AI Governance Framework for Generative AI**" (Generative AI Framework) for public consultation in January 2024.[231] A final version of the Framework was released in May 2024.[232] Building upon the IMDA's existing Model AI Governance Framework (Second Edition) launched in 2020, the Generative AI Framework identifies nine dimensions of generative AI governance: (1) accountability; (2) data; (3) trusted development and deployment; (4) incident reporting; (5) testing and assurance; (6) security; (7) content provenance; (8) safety and alignment R&D; and (9) AI for public good.

The Generative AI Framework provides recommendations and suggests areas for further study, such as allocating responsibility based on stakeholders' control in the AI development chain, updating legal frameworks for flexible redress, and implementing no-fault insurance schemes. It also addresses the application of personal data laws to generative AI, the potential of privacy-enhancing technologies, and the need for industry to coalesce around best practices in development and safety evaluation.

Other key initiatives include the following:

- Also in October 2023, the IMDA and the AI Verify Foundation released their Generative AI Evaluation Sandbox,[233] aiming to provide a common language for evaluating generative AI systems, develop a "body of knowledge" on testing generative AI products, and identify gaps in current assessment methods.
- In February 2024, the IMDA and Enterprise Singapore launched a Generative AI Sandbox for Small and Medium-sized Enterprises (SMEs).[234] The Sandbox aims to provide SMEs with practical experience in using generative AI solutions to enhance their marketing, sales, and customer engagement strategies.

---

[229] https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/nist-imda-joint-mapping-exercise

[230] https://aiverifyfoundation.sg/downloads/Discussion_Paper.pdf

[231] https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/public-consult-model-ai-governance-framework-genai

[232] https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/gen-ai-and-digital-foss-ai-governance-playbook

[233] https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/generative-ai-evaluation-sandbox

[234] https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/sg-first-genai-sandbox-for-smes

- In May 2024, the AI Verify Foundation released "Project Moonshot"[235] – an open-source toolkit for evaluating the security and safety of large language models (LLMs).

The PDPC has also addressed the use of personal data in AI systems through its Advisory Guidelines. In March 2024, the PDPC released its "**Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems**," following a public consultation from July to August 2023.[236] The Advisory Guidelines indicate how the PDPC would interpret the PDPA in the context of AI recommendation and decision systems. They outline appropriate legal bases under the PDPA for processing personal data by such systems, best practices for transparency, and responsibilities for third-party service providers developing and deploying "bespoke" AI systems.

## Privacy-Enhancing Technologies (PETs)

PETS have been a key priority for the PDPC since 2022, when the PDPC launched a PET Sandbox to support businesses who wish to pilot PET projects that address common business challenges.[237] In 2023 and 2024, the PDPC has taken steps to encourage the development and adoption of PETs through collaboration with industry.

- In July 2023, the IMDA launched a collaboration with Google on IMDA-Google: PET x Privacy Sandbox, a new initiative that aims to build on the IMDA's existing PET Sandbox by providing Singapore businesses with access to solutions from Google's Privacy Sandbox initiative.[238]

- The IMDA has published case studies arising from its ongoing PETs Sandbox,[239] including a case study from Meta and Mozilla on the use of Interoperable Private Attribution (IPA) for measuring digital advertising performance without the use of third-party cookies.[240] The case study was accompanied by recommendations from the PDPC on technical, governance, and process steps to lower the risks of re-identification.

- In July 2024, the PDPC commenced a public consultation on a new set of guidelines for generation of synthetic data, titled "**Privacy Enhancing Technology (PET): Proposed Guide on Synthetic Data Generation**."[241] Targeting tech leaders and data professionals, the draft guidelines seek to enhance understanding of synthetic data techniques and applications among organizations. To that end, the guidelines present use cases for synthetic data in AI training, data analysis, and software testing, and outline best

[235] https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/sg-launches-project-moonshot; https://aiverifyfoundation.sg/project-moonshot/

[236] https://www.pdpc.gov.sg/guidelines-and-consultation/2024/02/advisory-guidelines-on-use-of-personal-data-in-ai-recommendation-and-decision-systems

[237] https://www.pdpc.gov.sg/news-and-events/announcements/2022/07/launch-of-privacy-enhancing-technologies-sandbox

[238] https://www.pdpc.gov.sg/news-and-events/announcements/2023/07/new-joint-partnership-between-imda-and-google-to-help-singapore-businesses-prepare-for-a-privacy-first-future

[239] https://www.imda.gov.sg/how-we-can-help/data-innovation/privacy-enhancing-technology-sandboxes

[240] https://www.imda.gov.sg/-/media/imda/files/programme/pet-sandbox/imda-pet-sandbox--case-study--meta.pdf

[241] https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/proposed-guide-on-synthetic-data-generation.pdf

practices, including a five-step approach for generating synthetic data and methods to evaluate re-identification risks.

## Children's Privacy

In 2023 and 2024, the PDPC has increasingly turned its attention towards protecting children's privacy in the digital environment. These efforts demonstrate a strong commitment to safeguarding minors' personal data while balancing the need for data protection with the realities of the digital age.

In April 2024, the PDPC released its "**Advisory Guidelines on the Personal Data Protection Act (PDPA) for Children's Personal Data in the Digital Environment**"[242] following public consultation from July to August 2023. The Advisory Guidelines aim to protect minors in the digital age by requiring organizations that process children's data or have applications targeting or used by minors to adopt additional measures to protect children's data. The guidelines propose clarifying the PDPC's guidance on when organizations should seek parental consent for the use of minors' personal data and when higher standards for protecting children's personal data may apply.

In May 2024, the PDPC also updated Chapter 8 of its "**Advisory Guidelines on the PDPA for Selected Topics,**" which addresses Data Activities Relating to Minors, to align these with the April 2024 guidelines on children's personal data.[243]

In June 2023, the PDPC and IMDA launched an innovation challenge seeking to develop ways to assess individuals' ages (especially children) online without requiring the collection of facial images.[244] Participants will work with the PDPC, IMDA, organizations, and end-users to prototype privacy-preserving age estimation solutions and identify and address potential concerns.

## Data Portability

A right to data portability was introduced into the PDPA by the Personal Data Protection (Amendment) Act 2020.[245] However, this right is not yet operative and will only come into effect when the Singapore Government enacts relevant regulations.

---

242 https://www.pdpc.gov.sg/guidelines-and-consultation/2024/03/advisory-guidelines-on-the-pdpa-for-childrens-personal-data-in-the-digital-environment

243 https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/ag-on-selected-topics/advisory-guidelines-on-the-pdpa-for-selected-topics-(revised-may-2024).pdf

244 https://www.pdpc.gov.sg/news-and-events/announcements/2023/06/launch-of-the-pdpc-innovation-challenge

245 https://sso.agc.gov.sg/Acts-Supp/40-2020/

## International Cooperation

The PDPC actively engages with peer authorities in other jurisdictions. It is a member of the APPA Forum[246] and in recent years, has signed or renewed memoranda of cooperation with DPAs in Australia,[247] Hong Kong SAR,[248] Mexico,[249] and the Philippines.[250]

In April 2023, Singapore was appointed deputy chair of the Global Cross-Border Privacy Rules (CBPR) Forum,[251] a multilateral initiative that aims to promote the free flow of data, privacy, and data protection through the Global CBPR and Privacy Recognition for Processors (PRP) Systems.

The IMDA is also very active in the Association of Southeast Asia Nations (ASEAN). In February 2024, Singapore hosted the annual meeting of digital ministers from ASEAN member states, known as ADG-MIN, during which two key guidance documents were released: (1) the ASEAN Guide on AI Governance and Ethics; and (2) the Joint Guide to ASEAN Model Contractual Clauses and European Union Standard Contractual Clauses.[252]

246 https://www.appaforum.org/members/

247 https://www.pdpc.gov.sg/news-and-events/press-room/2023/12/singapore-signs-mou-with-mexico-and-renews-mou-with-australia-to-strengthen-personal-data-protection-efforts-globally

248 https://www.pdpc.gov.sg/news-and-events/press-room/2022/07/hong-kong-and-singapore-authorities-renew-mou-to-maintain-close-ties-and-foster-closer-collaboration-in-personal-data-protection

249 https://www.pdpc.gov.sg/news-and-events/press-room/2023/12/singapore-signs-mou-with-mexico-and-renews-mou-with-australia-to-strengthen-personal-data-protection-efforts-globally

250 https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/09/20220907jpcpsp

251 https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/singapore-appointed-as-deputy-chair-of-the-global-cross-border-policy-rules-forums-global-forum-assembly

252 https://www.pdpc.gov.sg/news-and-events/announcements/2024/02/two-guides-unveiled-at-adgmin-2024

# South Korea

A review of the Personal Information Protection Commission (PIPC)'s key strategic documents and recent regulatory actions reveals that its main priorities for 2024 include implementing amendments to the Personal Information Protection Act (PIPA), addressing privacy risks associated with AI, enhancing data portability, strengthening international cooperation on cross-border data transfers, and bolstering enforcement capabilities.

The PIPC has demonstrated a proactive approach to regulating emerging technologies, particularly AI, by issuing guidelines and establishing new regulatory frameworks. At the same time, its efforts to provide detailed guidance across various sectors and engagement with stakeholders through councils and committees also show a collaborative approach to regulation. The agency's increased investment in legal resources suggests a readiness to enforce regulations more assertively, especially against global tech companies.

As South Korea continues to position itself as a leader in the digital economy, the PIPC's role in shaping a trustworthy data protection landscape will be crucial. The outcomes of ongoing initiatives, such as the expansion of the MyData system and the development of AI-specific guidelines, will be critical in determining the effectiveness of South Korea's data protection framework in the coming years.

## Background

The PIPA[253] and its Enforcement Decree[254] provide the general legal framework for data protection in the Republic of Korea. The PIPA was enacted in 2011 and substantially amended in 2020 and 2023.

The PIPC is South Korea's national data protection authority, established on September 30, 2011.[255] The PIPC is an independent supervisory authority. It was elevated to a “central administrative agency” under the Prime Minister's Office in 2020, granting it the same status as South Korea's executive departments.

The PIPC is composed of nine commissioners: the Chairperson and Vice Chairperson (permanent) and seven non-permanent commissioners. The Chairperson holds a ministerial rank within the government. Commissioners are appointed by the President, with the Chairperson and Vice Chairperson recommended by the Prime Minister, and others recommended by the Chairperson, ruling party, and opposition parties. Commissioners serve a 3-year term. The current Chairperson is Dr. Hak-soo Ko (since 2022).[256]

253 http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95

254 http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95%EC%8B%9C%ED%96%89%EB%A0%B9

255 https://www.pipc.go.kr/np/default/page.do?mCode=F010010010

256 https://www.pipc.go.kr/np/default/page.do?mCode=F010040010

The PIPC's key functions include:

- developing policies on personal data protection;
- investigating and taking legal action against cases where personal data has been infringed;
- mediating and resolving personal data-related disputes and complaints;
- conducting research and education programs;
- raising awareness of personal data protection laws and policies;
- supporting technology development by disseminating information on personal data protection; and
- cooperating with international organizations and foreign personal information protection agencies.

The PIPA grants the PIPC broad investigatory and enforcement powers, ranging from recommendations to administrative fines. These powers are further complemented by a regime of criminal sanctions. The PIPC regularly publishes press releases on notable enforcement decisions on its website. It also publishes a casebook of key decisions interpreting the PIPA – the latest was published in December 2023.[257] The PIPC also regularly issues and updates guidelines to provide clear, up-to-date guidance for organizations on complying with their obligations under the PIPA obligations.[258]

It should be noted that in early September 2024, the PIPC allocated a total budget of KRW 64.6 billion (approximately US$48 million) for 2025.[259] This includes KRW 8.7 billion (approximately US$6.5 million) for research and development on PETs, KRW 2.4 billion (approximately US$1.8 million) for international cooperation (including hosting the Global Privacy Assembly in 2025), and KRW 12.1 billion (approximately US$9.1 million) for advancing the national MyData data portability initiative.

## Overview of Key Strategic Documents

The PIPC publishes several key strategic documents that outline its priorities and planned initiatives.

**Basic Plan for Personal Data Protection (2024-2026) (**개인정보 보호 기본계획 **(2024-2026), henceforth Basic Plan)**[260]

Article 9 of the PIPA requires the PIC to establish a Basic Plan for personal data protection every three years. The latest plan, published in June 2023, identifies ten priority areas for the PIPC's initiatives from 2023 to 2026.

| Priority | Key Actions |
|---|---|
| **1. Creating value with personal information to serve the public.** | • Encouraging and incentivizing Koreans to participate in the national data portability scheme, known as "**MyData**" (see below). |

[257] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=D010030000&nttId=9821#LINK
[258] For a full list of the PIPC's guidelines, see:
https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS217&mCode=G010030000
[259] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10525
[260] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS061&mCode=C010010000&nttId=8998#LINK

| | |
|---|---|
| | • Establishing the core legal and technological infrastructure to operationalize the MyData scheme.<br>• Ensuring that MyData is rolled out in a secure and organized manner. |
| **2. Creating a trusted environment for new technologies.** | • Advancing AI regulations while developing safeguards for personal data.<br>• Establishing baseline standards for automated decision making (ADM) to give effect to new data subject rights to request explanation and refuse AI-based automated decisions that can significantly impact their lives, such as those made in recruitment or welfare beneficiary selection processes (see below).<br>• Enabling research, development, and deployment of privacy-enhancing technologies (PETs).<br>• Developing regulations for use of biometric data. |
| **3. Promoting the safe use of personal data.** | • Expanding support techniques such as pseudonymization and anonymization.<br>• Creating frameworks for secure use of data, including establishing frameworks for generation of synthetic data.<br>• Supporting "Privacy Safe Zones" and regulatory sandboxes. |
| **4. Increasing protections for data subjects.** | • Improving the function of consent and data subject rights.<br>• Operating an effective dispute resolution system.<br>• Enhancing protections for vulnerable groups, including children, the elderly, and disabled. |
| **5. Strengthening public sector protections.** | • Strengthening safety measures for public-sector information.<br>• Introducing privacy assessment systems.<br>• Helping the government build trust in digital platforms. |
| **6. Supporting organizations' self-regulation efforts.** | • Promoting self-regulation through public-private partnerships.<br>• Establish monitoring and evaluation systems for private-sector self-regulation.<br>• Empowering Privacy Officers and fostering talent.<br>• Introducing and expanding Privacy by Design (PbD) certification programs. |
| **7. Strictly and promptly enforcing laws and systems.** | • Responding to new types of privacy infringements, such as manipulative design patterns.<br>• Enhancing remedies for data breaches and illegal distribution of personal data.<br>• Strengthening preliminary inspections of services.<br>• Participating in global joint investigations and enforcement. |

| | |
|---|---|
| **8. Creating a trusted environment for Koreans' data overseas.** | • Increasing interoperability of cross-border data transfer frameworks.<br>• Pushing for international data agreements.<br>• Strengthening the privacy of global platform companies. |
| **9. Promoting digital transformation.** | • Updating privacy principles, standards, and regulations, especially for data transfers and outsourcing.<br>• Developing safe protection for personal video information.<br>• Promoting alignment of South Korea's regulations with global standards. |
| **10. Becoming a global leader in privacy and data governance.** | • Researching risk-based and technology-neutral privacy schemes.<br>• Expanding privacy awareness through an ESG lens.<br>• Strengthening global collaboration and lead international consultations.<br>• Establishing a global privacy regulatory information hub.<br>• Helping companies comply with international regulations. |

**Annual Work Plan for 2024 (**개인정보보호위원회 **2024**년 업무계획**)**[261]

Article 10 of the PIPA requires the PIPC to publish an annual Work Plan indicating how it will implement the Basic Plan for the coming year. The latest plan, released in February 2024, outlines six core initiatives that the PIPC will pursue in 2024.

| Priority | Key Actions |
|---|---|
| **1. Creating conditions for the development of trustworthy AI.** | • Issuing guidelines on the application of the PIPA in several AI-related areas.<br>• Establish a regulatory sandbox for use of video data in mobility (e.g., self-driving cars).<br>• Establish Personal Data Safe Zones to provide AI researchers a secure environment for processing and using high-quality training data.<br>• Upholding data subjects' rights concerning ADM. |
| **2. Expanding data portability rights.** | • Supporting the implementation of the "MyData" service across domains and sectors that are closely related to people's daily lives, such as healthcare and telecommunications. |
| **3. Establishing a secure personal data protection system for everyday life.** | • Conducting proactive inspections in six key areas: (1) education and training services; (2) food delivery services; (3) information, broadcast and communication services; (4) smart cars; (5) AI and the metaverse, and (6) "super-apps", to increase data protection standards throughout society. |

[261] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS253&mCode=D080010020&nttId=9971; https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9921#LINK

| | |
|---|---|
| **4. Strengthening data subjects' rights in the digital age.** | • Implementing a scheme to assess organizations' privacy policies.<br>• Promoting protections for biometric data and vulnerable groups, including children and young people, including establishing a digital "right to be forgotten" for data subjects aged 29 and below. |
| **5. Creating and expanding a data protection ecosystem to support the digital economy.** | • Developing a new Personal Video Information Act to establish standards and safety measures for the use of video information by emerging technologies like self-driving cars and drones.<br>• Promoting the safe use of pseudonymized data and PETs.<br>• Developing standards in emerging fields like AI and blockchain.<br>• Establish a system to professionalize the chief privacy officer (CPO) role in certain large organizations. |
| **6. Engaging in international efforts to shape data protection standards.** | • Leading discussions on international data protection standards to promote interoperability with global data protection frameworks, especially for cross-border data transfers.<br>• Actively participating in global rulemaking on AI. |

**Annual Report for 2023 (2023년 개인정보보호 연차보고서)**[262]
Article 67 of the PIPA requires the PIPC to submit an annual report to the National Assembly. The latest report, released in October 2023, provides a detailed overview of the PIPC's activities and achievements during the period of January to December 2022.

# Key Priorities

## Legal Reform and Implementation

A major focus for the PIPC in 2023-2024 has been implementing amendments to the PIPA and its Enforcement Decree which took effect in September 2023.[263]

Key changes include:

- **Introducing a new data portability right** enabling data subjects to request that their data be transferred to themselves or third parties.
- **Introducing new ADM rights** enabling data subjects to request explanations for or reject: (1) fully automated decisions; and (2) automated decisions that substantially impact their rights and interests.
- **Unifying rules for online and offline service providers** and extending obligations previously only for online service providers to all data controllers.

[262] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS079&mCode=D070020000&nttId=9246
[263] https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2331

- **Introducing new legal bases for cross-border transfers** to jurisdictions with adequate protection levels or by certified controllers.
- **Empowering the PIPC to suspend cross-border data transfers** that are in breach of the PIPA or are to recipients with inadequate data protection standards.
- Replacing certain criminal sanctions with administrative penalties.
- **Increasing the maximum penalty under the PIPA** to 3% of *total* revenue, rather than *violation-related* revenue.

The majority of these amendments took effect in September 2023. However, certain provisions, such as the right to object to ADM, will take effect after a one-year grace period (i.e. in September 2024).

These amendments have informed several of the PIPC's activities in late 2023 and 2024, which are summarized below.

## Cross-Border Data Transfers

To support the implementation of the 2023 amendments, the PIPC established an Overseas Transfer Expert Committee in January 2024.[264] This 12-member committee will advise on matters relating to the PIPA's new cross-border data transfer mechanisms, including reviewing certification schemes and advising the PIPC on the adequacy of foreign jurisdictions' data protection frameworks.

## Data Portability

Implementing the "MyData" scheme is a key priority for the PIPC for the next two years. The MyData system has already been implemented in the financial and public sectors and is being progressively rolled out in other key sectors of South Korea's economy.

- In July 2023, the South Korean government established a team to implement the system and facilitate government-wide cooperation. Several South Korean ministries released a joint statement outlining their plan to roll out MyData gradually to 10 priority sectors by 2025.[265]
- In November 2023, the PIPC established and held the first meeting of the "Government-Wide MyData Consultative Council."[266] This Council is tasked with discussing and coordinating policy directions for the MyData initiative, including the design of the system and the implementation of pilot projects.
- From April to June 2024, the PIPC consulted on proposed amendments to the Enforcement Decree to implement MyData, with a view to a full-scale launch by the 2025 deadline. [267] The planned amendments focus on establishing detailed standards and procedures for transfer requests and transmission of personal data and outlining procedures for the PIPC to designate specialized institutions to facilitate the operation of the MyData scheme.

[264] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9887#LINK
[265] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9105#LINK
[266] https://www.korea.kr/briefing/pressReleaseView.do?newsId=156599647#pressRelease
[267] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10124#LINK

## AI

Throughout 2023 and 2024, the PIPC has adopted a proactive stance towards AI governance, ensuring that innovation does not come at the cost of privacy protection.

### AI Policy

In August 2023, the PIPC released a structured policy on its regulatory approach to AI titled "**Policy Direction for Safe Use of Personal Information in the AI Era**" (인공지능 시대 안전한 개인정보 활용 정책방향).[268] This policy serves as both a guidance document for complying with the PIPA when using personal data in AI systems and an overview of immediate actions that the PIPC would take to develop its AI capabilities, including:

- Establishing an **AI Privacy Team** to provide guidance on PIPA compliance for AI and develop AI data usage standards and an "**Public-Private Consultative Council for AI Privacy**" to create industry-specific guidelines through public-private collaboration.
- Launching a "**Prior Adequacy Review System**" by which the PIPC reviews a business's privacy practices before it launches an AI-driven service and helps the business to develop a PIPA compliance plan, in exchange for exemptions from certain penalties.
- Developing an **AI regulatory sandbox** with exemptions and deferrals to foster innovation.
- Developing **standards** for protecting personal data during development and deployment of AI services.

The PIPC has been quick to implement these actions, establishing the AI Privacy Team and Consultative Council in October 2023.[269] It also launched a pilot phase of the Prior Adequacy Review System in October 2023 and fully launched the System in March 2024.[270]

### Guidance

In its 2024 Work Plan, the PIPC indicated that it would issue guidelines on the application of the PIPA in six AI-related areas. To date, the PIPC has issued new guidelines on: (1) the use of visual data captured by mobile devices; [271] (2) use of pseudonymized personal data;[272] (3) synthetic data generation;[273] and use of publicly available data to train AI models.[274]

From May to June 2024, the PIPC consulted on a set of draft "**Standards for Measures on Automated Decisions**" (자동화된 결정에 대한 조치 기준) that organizations would be expected to follow when individuals exercise their

[268] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9083
[269] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9403
[270] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10023
[271] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=G010030000&nttId=9870
[272] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=G010030000&nttId=9900
[273] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=G010030000&nttId=10201
[274] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=G010030000&nttId=10375

rights to understand or challenge automated decisions introduced through the latest round of amendments to the PIPA.[275]

### Investigations

Between March and July 2023, the PIPC investigated ChatGPT over reports that the service had leaked personal data. The investigation resulted in a fine of KRW 3.6 million (approximately US$2,700) on OpenAI and identified several areas in which the company had failed to comply with the PIPA, including insufficient transparency, failing to observe the PIPA's consent provisions, and failing to obtain parental consent for users under the age of 14.[276]

Between November 2023 and June 2024, the PIPC conducted an investigation into major domestic and foreign AI service providers. The results of the investigation were published in two phases, with the first concerning large language models published in March 2024, and the second concerning AI-powered applications published in June 2024.

## Targeted Advertising

The PIPC has taken steps to address privacy concerns related to targeted advertising. In January 2024, the PIPC released a "**Policy Proposal for the Protection of Online Behavioral Information Used in Personalized Advertisements**" (맞춤형 광고에 활용되는 온라인 행태정보 보호를 위한 정책 방안).[277]

This proposal is the first step in a plan to revise the PIPC's existing guidelines to clarify the roles and responsibilities of key stakeholders, including businesses that use behavioral data to serve personalized advertisements, third parties that provide advertising space, and operators that manage in-app browsers. It aims to balance the interests of businesses in using behavioral information for personalized advertising with the need to protect individuals' privacy rights.

## Children's Privacy

While children's privacy has been less of a priority for the PIPC in 2023 compared with previous years, it remains an area of focus. In July 2022, the PIPC, together with other South Korean ministries, released a "**Basic Plan for the Protection of the Personal Information of Children and Youth**" (아동·청소년 개인정보 보호 기본계획).[278] This plan aims to ensure that children's personal information is protected in digital environments while also creating conditions that empower children to make decisions about their personal information and exercise their rights.

[275] https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000%22&nttId=10174
[276] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9055#LINK
[277] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9888
[278] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=8136

Since enacting the Basic Plan, the PIPC's focus has shifted to providing children with a "**Digital Right to be Forgotten**." In April 2023, the PIPC launched an "Eraser Service," which enables children to request removal of online content containing their personal data.[279]

## Enforcement

The PIPC actively enforces the PIPA. The latest figures on the PIPC's patterns of enforcement are found in the 2023 Annual Report. During 2022, the PIPC imposed corrective measures against 146 private-sector entities. This includes:

- Issuing 112 fines which collectively totaled KRW 598.8 million (approximately US$440,700);
- Imposing other financial 17 penalties totaling KRW 1,018.289 billion (approximately US$789.5 million);
- Issuing corrective orders and recommendations to 42 entities; and
- Publicizing 48 infringements of the PIPA.

The PIPC's enforcement powers have been strengthened following the 2023 amendments to the PIPA. Since the amendments took effect, the PIPC has taken further steps to strengthen its enforcement capabilities. In January 2024, the PIPC announced that it had secured a litigation budget of 420 million won (approximately US$315,000) to respond proactively to administrative lawsuits involving global "Big Tech" companies in 2024.[280] The PIPC has continued its active approach to enforcement throughout 2024, imposing fines in excess of US$11 million on as Kakao[281] and US$5 million violations on Golfzon[282] for failing to secure personal data.

## Ecosystem Building

The PIPC has taken steps to build a robust data protection ecosystem in South Korea. In April 2024, the PIPC and the Korea Internet and Security Agency (KISA) awarded South Korea's first certification for "Privacy by Design" (PbD).[283] This initiative aligns with PIPC's goal outlined in its Basic Plan 2023-2026 to protect South Korean citizens from data breaches by establishing a PbD certification system for digital devices collecting sensitive data.

In July 2024, the PIPC announced the implementation of a simplified system for small and medium-sized enterprises (SMEs) to obtain certification under the Information Security and Personal Information Management System (ISMS-P).[284] This new system aims to address challenges faced by SMEs, including the ISMS-P's extensive requirements and the high costs of certification.

The PIPC also announced the establishment of the Korea Privacy Officers Association (KPA) in July 2024.[285] This organization represents data protection officers (DPOs) from both public and private sectors and aims to enhance collaboration among DPOs and improve communication with the government on data protection policies.

[279] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9887#LINK
[280] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9869
[281] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10180#LINK
[282] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10158
[283] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10090
[284] https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10379#LINK
[285] https://m.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10387#LINK

## International Cooperation

The PIPC actively participates in international forums and cooperates with data protection authorities from other countries. It is a member of the Global CBPR Forum, APPA Forum, and the GPA. These engagements demonstrate the PIPC's commitment to aligning South Korea's data protection practices with global standards and contributing to international discussions on data protection and privacy.

# Thailand

Thailand's Personal Data Protection Act (PDPA), which came into full effect on June 1, 2022 after a series of COVID-19 related delays, marks a significant milestone in the country's data protection landscape. Since the law's implementation, the Office of the Personal Data Protection Commission (PDPC), established in January 2022 to administer and enforce the PDPA, has focused on providing guidance, raising awareness, and engaging in rulemaking to operationalize the law's provisions. This has included issuing subordinate regulations and guidelines on key aspects such as cross-border data transfers, data breach notification, and the appointment of Data Protection Officers (DPOs).

More recently, the PDPC has shifted its attention towards strengthening enforcement of the PDPA. This is reflected in the PDPC's strategic priorities, as outlined in its inaugural Master Plan for 2024-2027, which emphasizes effective PDPA enforcement, enhancing knowledge and trust in the law, promoting Thailand's digital economy, and advancing research and development in personal data protection. The PDPC's enforcement actions in late 2023 and early 2024, such as decisions against a Thai insurance company for PDPA violations and summoning the Japanese messaging app LINE for investigation, further demonstrate this shift towards more stringent enforcement.

## Background

Thailand's PDPA[286] was passed in May 2019 but faced several postponements (due mainly to the COVID-19 pandemic) before coming into full effect on June 1, 2022. The PDPA serves as the primary legislation governing personal data collection, use, and disclosure in Thailand.

To oversee the implementation and enforcement of the PDPA, the PDPC[287] was formally established on January 18, 2022. The PDPC is chaired by Thienchai Na Nakorn and consists of the Chairperson, Vice-Chairperson, five commission members, and nine honorary commission members.[288] The PDPC's mandate, as outlined in Chapters IV and V of the PDPA, includes:

- Developing a master plan for personal data protection;
- Issuing necessary notifications and rules to implement the PDPA;
- Providing advice and consultancy on personal data protection;
- Conducting investigations and appointing expert committees to handle complaints and PDPA violations;
- Imposing administrative fines of up to 5 million THB (approximately US$139,000) for PDPA violations.

[286] https://www.pdpc.or.th/1561/
[287] https://www.pdpc.or.th/
[288] https://www.pdpc.or.th/about-pdpc/pdpc-structure/

Under the PDPA, the PDPC may also establish expert committees to consider complaints under the PDPA, investigate acts relating to personal data, resolve disputes, and perform other tasks assigned by the PDPC.

## Overview of Key Strategic Documents

The PDPC's strategic objectives and priorities are outlined in two key documents:

**Master Plan for the Promotion and Protection of Personal Data 2024-2027 (Master Plan)**
**(แผนแม่บทการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลของประเทศ พ.ศ. 2567 – 2570)**
Published on April 29, 2024, the PDPC's inaugural Master Plan comprehensively sets out the PDPC's data protection strategies from 2024 to 2027, highlighting areas of alignment with Thailand's broader national strategies.[289] The Master Plan outlines 4 strategic priorities for the PDPC during this period:

1. **Effective and balanced enforcement of the PDPA**: The PDPC aims to develop standards, rules, and tools to strengthen personal data protection and ensure PDPA compliance among government agencies, listed companies, and SMEs. This includes providing guidelines, promoting Trust Mark certification, and implementing compliance inspection mechanisms.
2. **Enhancing knowledge of, and trust, in the PDPA**: To foster a culture of data protection, the PDPC seeks to enhance PDPA knowledge and trust through awareness-raising campaigns, targeted learning mechanisms, and increasing the number of Data Protection Officers (DPOs). This involves developing standard training courses, improving media and digital literacy, and creating sustainable learning models.
3. **Promoting the digital economy and society**: Recognizing the importance of data protection in the digital age, the PDPC aims to promote Thailand's digital economy by improving its Privacy Index ranking, increasing investment in the digital industry, and reducing personal data protection violations. This will be achieved through collaboration with stakeholders and adding value to industries.
4. **Research and development**: To drive innovation in personal data protection, the PDPC plans to create a research ecosystem for privacy-preserving solutions, enhance competitiveness, and encourage technology adoption. Key initiatives include establishing sandboxes, academic and research networks, upgrading PDPA services, and organizing an international PDPA Summit.

The Master Plan also outlines a three-phase action plan for each strategy, along with indicators, sub-strategies, and the roles of lead and supporting agencies. It discusses the mechanisms for implementing the plan, including resource management, collaboration with cooperation networks, and a monitoring and evaluation framework.

**Annual Performance Report for the Office of the Personal Data Protection Committee (Annual Report)**
**(รายงานประจำปี 2566)**
The PDPC's Annual Report provides a detailed account of the commission's activities, budget allocations, and operational outcomes for the year.[290] In 2023, the PDPC had an annual budget of 80,346,000 THB (approximately US$2,195,000), which was used to support its various initiatives and functions.

[289] https://www.pdpc.or.th/5448/
[290] https://www.pdpc.or.th/pdpc-book/anual-report-2566/

In addition to these key documents, the PDPC regularly publishes announcements, press releases, and leaflets on its website[291] and Facebook page[292] to provide guidance, raise awareness, and keep stakeholders informed about the latest developments in personal data protection.

# Key Priorities

## Enforcement

Strengthening PDPA enforcement is a key strategic priority for the PDPC, as outlined in its Master Plan. The PDPC aims to develop compliance mechanisms, enhance regulatory capabilities, and continually improve the legal framework to keep pace with technological advancements and emerging privacy challenges. In June 2023, the PDPC published a notification detailing the procedure for the Expert Committee to issue administrative orders Establishing the PDPA Center to monitor and receive non-compliance complaints (January 2024).

While enforcement was relatively relaxed in the initial months following the PDPA's implementation to allow for awareness and compliance to increase, the PDPC's actions in late 2023 and early 2024 suggest a shift towards more stringent enforcement. On October 17, 2023, the PDPC announced that the Expert Committee had, for the issued its first enforcement decision in a case concerned unauthorized use of personal data by an insurance company.[293]

Since then, the PDPC has taken an increasingly proactive stance toward enforcing the PDPA. In August 2024, the PDPC issued its largest fine to date (7,000,000 THB or approximately US$210,000) following a breach of the personal data of over 100,000 customers of an online retail company.[294] Key violations identified by the PDPC's Expert Committee include:

- Failure to appoint a DPOData Protection Officer as required by PDPA, despite handling large volumes of customer data.
- Lack of appropriate security measures, leading to the data breach.
- Ignoring customer complaints about the data leak and failing to report the incident to the PDPC within the legally mandated time frame.

The PDPC also ordered the company to improve its security measures, conduct staff training, and report on corrective actions taken.

---

[291] https://www.pdpc.or.th/
[292] https://www.facebook.com/PDPC.TH
[293] https://www.facebook.com/photo/?fbid=343092681564829&set=pcb.343092914898139
[294] https://www.mdes.go.th/news/detail/8539-%E0%B8%94%E0%B8%B5%E0%B8%AD%E0%B8%B5---%E0%B8%AA%E0%B8%84%E0%B8%AA--%E0%B8%84%E0%B8%B8%E0%B8%A1%E0%B9%80%E0%B8%82%E0%B9%89%E0%B8%A1%E0%B8%AA%E0%B8%B1%E0%B9%88%E0%B8%87%E0%B8%9B%E0%B8%A3%E0%B8%B1%E0%B8%9A%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%A3%E0%B8%B1%E0%B9%88%E0%B8%A7%E0%B9%84%E0%B8%AB%E0%B8%A5%E0%B8%A0%E0%B8%B2%E0%B8%84%E0%B9%80%E0%B8%AD%E0%B8%81%E0%B8%8A%E0%B8%99-%E0%B8%88%E0%B8%B3%E0%B8%99%E0%B8%A7%E0%B8%99-7-%E0%B8%A5%E0%B9%89%E0%B8%B2%E0%B8%99%E0%B8%9A%E0%B8%B2%E0%B8%97

## Rulemaking

Since its establishment, the PDPC has actively engaged in rulemaking to clarify PDPA provisions and facilitate compliance. This process has continued through 2023 and 2024, with the PDPC issuing numerous subordinate regulations and guidelines addressing key areas such as:

- Cross-border data transfers under Sections 28 and 29 of the PDPA;[295]
- Appointment and responsibilities of DPOs;[296]
- Security measures for personal data protection;[297]
- Processing of sensitive data, such as criminal records;[298] and
- Processing personal data for archiving and research purposes.[299]

These regulations and guidelines provide much-needed clarity for businesses and organizations, helping them understand their obligations under the PDPA and implement appropriate measures to protect personal data.

## Cross-Border Data Flows

The PDPC has been actively developing its cross-border data transfer framework throughout 2023. In December 2023, the PDPC issued the final version of its regulations for cross-border data transfers under Sections 28 and 29 of the PDPA.[300] These notifications provide clarity on adequacy decisions, Binding Corporate Rules, and the use of Standard Contractual Clauses (SCCs), such as the ASEAN Model Contractual Clauses and the European Commission's Standard Contractual Clauses. These regulations took effect in March 2024. Going forward, we expect that the PDPC will shift its focus to enforcing these provisions. It may also begin issuing adequacy decisions within the new framework.

## International Cooperation

Although not currently an active contributor to international data protection forums, the PDPC recognizes the importance of international cooperation in establishing globally recognized personal data protection standards. The Master Plan identifies cooperation with international organizations such as APEC, ASEAN, OECD, and ITU as an opportunity for Thailand to engage in Free Trade Agreements and Digital Economy Partnership Agreements (DEPA).

[295] https://www.pdpc.or.th/2500/; https://www.pdpc.or.th/2507/
[296] https://www.pdpc.or.th/2384/
[297] https://www.pdpc.or.th/2271/; https://www.pdpc.or.th/2971/
[298] https://www.pdpc.or.th/2564/
[299] https://www.pdpc.or.th/2557/
[300] https://www.pdpc.or.th/2500/; https://www.pdpc.or.th/2507/

To foster knowledge sharing and collaboration, the Master Plan proposes organizing an international PDPA Summit, which would bring together stakeholders from various countries to discuss advancements and best practices in personal data protection.


Washington, DC | Brussels | Singapore | Tel Aviv

info@fpf.org

FPF.org