ISSUE BRIEF

GLOBAL

# Keeping up with “Consent” in Data Protection Frameworks:

## A Comprehensive Update for APAC

Author: Sakshi Shivhare
Editors: Dominic Paulger and Bianca-Ioana Marcu
April 2025

FUTURE OF PRIVACY FORUM

# Table of Contents

# Keeping up with "Consent" in Data Protection Frameworks:

## A Comprehensive Update for APAC

Author: Sakshi Shivhare, FPF, April/2025

## Introduction

Many jurisdictions in the Asia-Pacific (APAC) region rely heavily on consent as the primary basis for processing of personal data. In a previous research, conducted between September 2021 and November 2022, we analyzed the lawful grounds for processing in 14 data protection frameworks in the region (Australia, China, India, Indonesia, Hong Kong SAR, Japan, Macau SAR, Malaysia, New Zealand, the Philippines, Singapore, South Korea, Thailand, and Vietnam). Although the resulting comparative report identified twenty-six distinct alternative legal bases across the jurisdictions, it found that organizations often find these alternatives difficult to use for various needs, such as cross-border compliance programs, due to their limited availability, stringent requirements, or narrow scope. Consequently, businesses operating in these jurisdictions have predominantly centered their compliance programs on obtaining consent. However, this reliance is not ideal for several reasons:

- Scaling consent processes can be challenging, particularly for small organizations with limited resources.
- The practice of obtaining consent can often be reduced to a mere checkbox exercise, which fails to promote genuine accountability to data subjects.
- Most critically, the overuse of consent has led to "consent fatigue" among data subjects, where individuals become desensitized to frequent consent requests. This phenomenon diminishes the effectiveness and meaningfulness of consent, ultimately undermining the very protection of personal data that consent mechanisms are intended to ensure.

The landscape for privacy and data protection in APAC is far from static, and presents notable developments with regard to consent requirements. Since the publication of the fourteen jurisdictional reports (2022 reports), there have been significant changes to the privacy and data protection landscape in the region.

In particular, some jurisdictions have enacted **new data protection laws**:

- In August 2023, **India** enacted the Digital Personal Data Protection Act, 2023 (DPDPA), which will come into force once the government notifies an effective date.
- In April 2023, **Vietnam** introduced the Decree on Personal Data Protection (Decree), effective from 1 July 2023.

- In October 2022, **Indonesia** enacted the Personal Data Protection Law (PDPL), Act No. 27 of 2022, effective from 17 October 2022, with a two-year transition period for organizations.

Others have issued **new guidelines** interpreting the legal bases for processing personal data under their existing data protection laws:

- In November 2023, **the Philippines** issued a Circular for Guidelines on Consent, which provides significant clarification and guidance on the use of consent as a lawful basis for processing personal data.

- In March 2022, **South Korea** introduced two sets of guidelines–"Easy-to-Understand Manual on Consent for Personal Data Processing" and "Guidelines for Writing Privacy Policies."

- In October 2024, the Office of the Australian Information Commissioner (OAIC) issued two sets of guidelines addressing privacy considerations in AI in **Australia**–"Guidance on privacy and developing and training generative AI models" and "Guidance on privacy and the use of commercially available AI products."

And some have **amended their data protection laws**:

- In September 2023, significant amendments to **South Korea**'s Personal Information Protection Act (PIPA) took effect; and in January 2025, a bill seeking to expand the available legal bases to process personal data under the PIPA for the development of artificial intelligence (AI) was introduced in the National Assembly.

- In July 2024, **Malaysia**'s Parliament passed the Personal Data Protection (Amendment) Bill 2024, and in October 2024, the Personal Data Protection (Amendment) Act 2024 was published in Malaysia's Federal Gazette after receiving Royal Assent on 9 October 2024.

- In December 2024, **Australia**'s Parliament passed the Privacy and Other Legislation Amendment Act 2024, giving effect to several proposed amendments to Australia's Privacy Act raised in a multi-year legislative review.

Within this context, this Issue Brief summarizes the key developments since the 2022 reports and provides insights into the evolving consent requirements and alternative legal bases for data processing in the APAC region. By bridging the gap between the 2022 reports and the current state of affairs, we note significant trends and challenges in the rapidly evolving data protection landscape across key APAC jurisdictions.

For completeness, the Issue Brief also summarizes amendments to Malaysia's and Australia's data protection laws that were recently enacted. However, these amendments do not affect the requirements for consent or alternative legal bases to process personal data.

## Emerging Trends and Challenges in the APAC Data Protection Landscape

**The APAC region is undergoing a significant transformation in data protection, transitioning from fragmented, sector-specific regulations to unified frameworks**, as seen with recent legislative changes in India, Vietnam, and Indonesia. This shift towards harmonization presents challenges in aligning new laws with existing regulations and international standards, requiring careful consideration of local nuances to ensure effective global compliance.

**Consent remains fundamental to data protection in APAC, but awareness of its limitations is growing, leading to the adoption of additional legal bases for data processing in new or updated frameworks**. Jurisdictions such as Indonesia now recognize alternatives such as legitimate interests, contrasting with countries such as China and Malaysia, which continue to rely on consent as the primary legal basis. This evolving landscape aims to balance individual rights with data processing needs for business and societal functions. For example, new regulations in India, Indonesia, and Vietnam are expanding legal bases beyond consent, providing businesses with greater flexibility. However, this also introduces challenges in ensuring that these broader legal bases are implemented with adequate safeguards.

**The rise of AI development is beginning to catalyze a shift away from strict consent-based models in some jurisdictions, while others apply existing frameworks to this new technological context.** South Korea's proposed PIPA amendment facilitates the use of personal data for AI development beyond the original purpose of collection, while Japan's data protection authority is also considering proposals to relax consent requirements for AI development. In contrast, Australia's recent AI guidelines apply the Privacy Act's existing Australian Privacy Principles to AI contexts without altering the fundamental legal bases for data processing. This divergence highlights regional variations in addressing AI's unique privacy challenges, with some jurisdictions creating AI-specific exemptions while others adapt existing frameworks.

**Efforts are also underway to make consent mechanisms more user-friendly.** The Philippines addresses "consent fatigue" in its guidelines, South Korea aims to clarify the consent process in its guidelines, and India has introduced "consent managers" in its data protection law. These initiatives exemplify efforts to empower data subjects and enhance transparency in data handling practices. As this trend towards increased transparency gains momentum, organizations will be challenged to refine their practices to balance legal compliance with clear and effective communication to users.

In addition, **there is an increased focus on the protection of sensitive personal data and vulnerable groups, especially children**. For example, India will require verifiable consent of a parent or guardian, while Vietnam necessitates verification of a child's age by all parties involved to ensure compliance. The challenge is to apply these protections consistently across different cultural and legal frameworks, ensuring that safeguards are effective yet adaptable.

Finally, **stronger enforcement mechanisms and significant penalties for non-compliance are becoming more common**, emphasizing the importance of complying with data protection laws. While this increases the effectiveness of data protection regulations, it also presents challenges for organizations, particularly in terms of compliance costs and potential liabilities, underscoring the need for careful planning and resource allocation.

## Key Findings from Recent Developments in the APAC Region

**India, Vietnam, and Indonesia have significantly consolidated their previously fragmented regulatory approaches, with consent remaining central to their data protection frameworks.** However, these jurisdictions are evolving their approach to consent to improve transparency, specificity, and the ease of withdrawal. India's DPDPA introduces "consent managers," innovative intermediaries designed to help individuals efficiently manage their consent across various data fiduciaries (equivalent to a "data controller" under the EU's General Data Protection Regulation (GDPR)), potentially setting a precedent for other jurisdictions.

**While consent maintains its primacy, several jurisdictions have introduced alternative legal bases for data processing**. India's DPDPA introduces "certain legitimate uses," even if they are narrow in scope, Vietnam's Decree outlines specific situations in which processing without consent is permitted, and Indonesia's PDPL recognizes alternatives similar to the GDPR, including legitimate interests. In addition, the Philippines has taken steps to clarify the use of legitimate interests as a legal basis and has issued detailed guidance on its application.

**The protection of sensitive data and children's data has received particular attention in these jurisdictions.** More stringent requirements for the processing of sensitive personal data are common, and specific provisions for obtaining consent for the processing of children's data have been introduced, albeit with different age thresholds in different countries. Cross-border data transfers are also a focus, with regulations requiring additional safeguards beyond mere consent to ensure data protection across borders.

It is important to note that **many of these jurisdictions are in transition periods or awaiting further implementing regulations**. Regulators are actively issuing guidance to clarify requirements and facilitate compliance, indicating that the landscape continues to evolve.

## Developments on the Horizon in APAC

Several significant developments are underway across the APAC region that will further shape approaches to consent requirements and alternative legal bases for processing personal data. While some of these changes are

in advanced stages of development, others are still evolving, and their final form may be subject to modification through ongoing consultative or review processes:

**In India, following the public consultation on the draft Digital Personal Data Protection Act (DPDPA) Rules** (draft Rules) **that concluded in March 2025, the final Rules are expected to be published by the end of 2025.** The draft Rules aim to operationalize critical provisions of the DPDPA, including requirements for notice, parental consent for processing children's data, breach notifications, and the establishment of the Data Protection Board. The extent of revisions in the final Rules will likely vary based on how the Ministry of Electronics and Information Technology (MeitY) integrates the feedback received during the consultation process.

**Vietnam is moving toward enacting a comprehensive national data protection law, with an updated draft Law on Personal Data Protection (draft Law) currently under consideration.** On 24 September 2024, the Vietnamese government released the first draft of this comprehensive law for public feedback. Subsequently, in March 2025, an updated version was unofficially released. Following deliberations at the National Assembly's 7th Session in March 2025, the draft Law has been referred for further refinement before submission at the upcoming 9th session. The draft Law, which builds upon the existing Decree, maintains consent as a primary basis for data processing while also recognizing alternative legal bases such as contractual necessity, legal obligations, vital interests, public interest, and state emergencies.

**South Korea's National Assembly is considering a bill, introduced on 31 January 2025, that would expand the legal bases available under the PIPA for processing personal data for AI development.** The key change introduced by the bill is the new Article 28.12, which permits the use of personal information beyond its original purpose of collection for development and improvement of AI systems, provided that the following conditions are met: (1) the nature of the data must be such that anonymizing or pseudonymizing it would make it difficult to use in AI development; (2) appropriate technical, administrative, and physical safeguards must be implemented; (3) the purpose of AI development must align with objectives such as promoting public interest, protecting individuals or third parties, or fostering AI innovation; and (4) there must be minimal risk of harm to data subjects or third parties. This legislation could serve as a reference for other APAC jurisdictions looking to support AI development, particularly as AI development increasingly relies on large datasets that often include personal data.

**Japan's Personal Information Protection Commission (PPC) is expected to finalize its proposals for reforms to its data protection law, the Act on the Protection of Personal Information (APPI), as part of its ongoing review.** The PPC plays a crucial role in shaping potential amendments to the APPI and is required to review the APPI every three years to ensure that the legislation remains up-to-date with developments in technology and data protection. The PPC commenced its current review of the APPI in November 2023. On 5 March 2025, the PPC published a package of potential amendments to the APPI, including proposals to relax consent requirements for processing personal data, and enhance protections for children's personal data, including by introducing parental consent requirements. One of the key aspects of the potential proposals includes allowing the processing of personal information without consent for the creation and use of statistical information, which explicitly includes AI

development that can be organized as statistical preparation, provided that certain conditions are met. It remains to be seen to what extent these proposals will be translated into a bill to amend the APPI.

**New Zealand's Privacy Amendment Bill, which passed its second reading in February 2025, is progressing through Parliament.** The Bill introduces a new Information Privacy Principle (IPP 3A) requiring organizations to notify individuals when collecting their personal information from third-party sources, subject to specific exceptions. If enacted, this provision would apply to personal information collected on or after 1 June 2025.

*Several other important developments that would shape the broader data protection landscape in the APAC region include:*

With Indonesia's general election concluded in 2024, the new **Indonesian government is expected to enact key regulations implementing the country's Personal Data Protection Law (PDPL)**. Despite the PDPL coming into effect in October 2022, there remains a lack of clarity on crucial issues, including the establishment of a data protection authority to enforce the law. In August 2023, Indonesia's Ministry of Communications and Information Technology (KOMINFO) published the Draft Government Regulation (GR Draft) on the implementation of the PDPL for public discussion and consultation. Inter alia, the GR Draft elaborates on the scope of authority vested in the institution responsible for the implementation of the PDPL under Article 58. In March 2024, KOMINFO announced the formation of an Inter-Ministerial Committee to finalize the regulations, aiming to submit the final version for Presidential ratification by July 2024. As of April 2025, there have been no further updates regarding the Presidential ratification of these regulations.

**Malaysia's data protection framework will continue to develop throughout 2025 following the enactment of amendments to the Personal Data Protection Act 2010.** Malaysia's Personal Data Protection Department (PDPD) has already issued guidelines on the appointment of Data Protection Officers and data breach notifications, with additional guidelines expected on data portability, cross-border transfers, and security standards. The PDPD has announced that the implementation of these amendments will proceed in three phases, with the final phase introducing significant new provisions starting 1 June 2025.

**Australia is expected to advance its second tranche of amendments to the Privacy Act 1988, with consultations anticipated in 2025 and a second amendment bill likely before the end of 2025.** This second tranche may include several contentious and more ambitious reforms that were deferred from the first tranche, such as removing the small business exemption, changing the handling of employee records data, introducing a right to erasure, implementing a new "fair and reasonable" test for information handling, and ending reliance on "implied consent" for data collection. However, it remains to be seen whether these reforms, which have been led by the incumbent Labour Government, will survive the upcoming 2025 federal election, which is scheduled for May 2025.

**Hong Kong, which has been working on amendments to its Personal Data (Privacy) Ordinance (PDPO) since 2020, is expected to make progress on these amendments with potential legislative proposals emerging in 2025.** In April 2024, a senior Hong Kong official informed Hong Kong's Legislative Council that the government

was working with the Office of the Privacy Commissioner for Personal Data (PCPD) to propose amendments to the PDPO in several key areas, including establishing a mandatory data breach notification mechanism, requiring the formulation of data retention policies, empowering the Privacy Commissioner to impose administrative fines, directly regulating personal data processors, and clarifying the PDPO's definition of "personal data." Considering that the PDPO has only been amended twice since its enactment in 1995 (in 2012 and 2021), these upcoming amendments would represent a significant update to Hong Kong's data protection framework.

Having explored the developments on the horizon across key APAC jurisdictions, we now take a deep dive into each jurisdiction's approach to consent requirements and alternative legal bases for data processing.

## India

India's journey towards a comprehensive data protection law has been long and complex, culminating in the Digital Personal Data Protection Act, 2023 (DPDPA). Enacted on 11 August 2023, this landmark legislation marks a significant milestone in India's approach to data protection, replacing the previous patchwork of regulations with a unified framework, as explained in FPF's blog post on the DPDPA. The DPDPA will take effect when the government notifies an effective date. Once its provisions take effect, the DPDPA will supersede Section 43A of the Information Technology Act, 2000, and the associated SPDI Rules, 2011, which currently govern private-sector entities handling sensitive personal data.

At the core of the DPDPA are two fundamental legal bases for processing personal data: consent and certain legitimate uses. This approach provides flexibility while ensuring that data principals (equivalent to "data subjects" under the GDPR) remain in control of their information. However, the severe penalties for non-compliance underscore the need for organizations to be vigilant in their data protection practices. It details specific requirements for the validity of consent and introduces innovative mechanisms, such as consent managers, to facilitate consent management.

1. ***The DPDPA permits the processing of personal data under two legal bases: "consent" and "certain legitimate uses."***

   While consent is the primary basis for lawful processing of personal data, certain specific grounds permit processing personal data without consent. As per Section 4, data fiduciaries can process personal data only for a lawful purpose, either with the consent of a data principal for a specific purpose or by identifying a certain legitimate use.

1.1. **Express conditions for consent require it to be freely given, obtained through clear affirmative action, and easily withdrawable.** As stipulated by Section 6 of the DPDPA, consent must also be specific, informed, unconditional, and unambiguous, indicating the data principal's agreement to process their

data solely for specified purposes. Section 6(4) guarantees data principals the right to withdraw consent at any time, with the withdrawal process mandated to be as straightforward as granting consent.

- Data fiduciaries must give data principals a notice in plain language before or at the same time as seeking consent. The notice must be accessible in English or any language listed in the Constitution of India. Section 5(1) specifies the details to be included in the notice.
- Moreover, it requires data fiduciaries to promptly update the consents obtained before the enactment of the DPDPA with the requirements mentioned above.

1.2. The processing of **personal data of children** (below 18 years) and individuals with disabilities mandates verifiable consent from a parent or legal guardian, with specific methods for obtaining this consent to be detailed in forthcoming implementing rules.

1.3. **The DPDPA does not require separate consent for cross-border data transfers.** The DPDPA empowers the Central Government to restrict transfers to specific countries or territories by notification, and all obligations applicable to local data transfers within India apply equally to cross-border data transfers, including obtaining consent from data principals or utilizing legitimate uses.

2. ***The DPDPA introduces "consent managers," a new category of entities designed to help data principals provide, manage, review, and withdraw their consent efficiently.***

Operating as centralized intermediaries, "consent managers" streamline the consent process through an accessible, transparent, and interoperable platform and are required to be registered with the Data Protection Board of India (Board), which is yet to be established. Consent managers are accountable to the data principal and operate on their behalf. The Central Government guidance is anticipated to provide further clarity on the specific responsibilities and duties of consent managers.

The concept of consent managers in data protection law is unique internationally, however, India already has a similar concept in its financial sector, introduced by the Reserve Bank of India (India's central bank and regulatory body responsible for regulating the Indian banking system). The RBI's "Master Direction–Non-Banking Financial Company–Account Aggregator (Reserve Bank) Directions, 2016" established "account aggregators" as data intermediaries. These entities collect and share financial information from various financial information providers to financial information users, only with the consent of the consumer. Officially set up in 2021, the role of these account aggregators mirrors that of consent managers in managing personal data.

3. ***The DPDPA provides "certain legitimate uses" as an alternative basis for processing personal data without the data principal's consent.***

Similar to the GDPR, the DPDPA ensures that data processing is tied to specific, lawful purposes, with alternative legal bases that include compliance with legal obligations, protection of individuals' vital

interests, and processing in the public interest. Despite some commonalities, a significant difference is that, unlike the GDPR, the DPDPA does not recognize "legitimate interests" or "contractual necessity" as legal bases for processing. This absence of "legitimate interests" in the DPDPA is consistent with data protection laws in China, Malaysia, and Vietnam. In contrast, at least ten other APAC jurisdictions feature more flexible data protection laws that potentially consider "legitimate interests" or its equivalents.

Under the DPDPA, "certain legitimate uses" serve as the only alternative to consent, providing data fiduciaries with narrow options to process personal data without consent and reducing flexibility for routine operations. Notably, this provision lacks the broader "legitimate interests" basis and corresponding balancing test against data subject rights found in the GDPR. Although earlier drafts of the DPDPA included "reasonable purposes" as a basis for processing, which could encompass legitimate interests, this was excluded in the final version.

Key differences between the DPDPA and the GDPR reflect the different legal and cultural contexts of India and the EU. The DPDPA specifies nine precise scenarios under "certain legitimate uses," while the GDPR categorizes processing into five broad categories. The DPDPA emphasizes government and state-related processing, emergencies, breakdown of public order, and health threats, thus addressing India's unique needs. In contrast, the GDPR addresses government processing more generally under the public interest.

In addition, the DPDPA includes a provision for employment-related processing, which is not as explicitly covered by the GDPR.

4. ***The DPDPA authorizes the Board to impose a monetary penalty up to INR 2.5 billion (approx. USD 30 million) for significant breaches of its provisions.***

Section 33 of the DPDPA reinforces the importance of adhering to legal bases for data processing by detailing penalties for "significant" breaches, indicating a risk-based approach to enforcement. Factors such as the nature, gravity, and duration of the breach, and the type of data affected, are considered when determining penalties. Breaches involving sensitive data or lacking a clear legal basis may be considered more serious, encouraging data fiduciaries to carefully justify their data processing activities. This penalty provision serves as the enforcement backbone of the DPDPA, ensuring compliance with legal bases and maintaining the effectiveness of the overall data protection framework.

## Vietnam

On 17 April 2023, Vietnam introduced the Decree of Personal Data Protection (Decree), addressing the previously fragmented legal framework governed by nineteen different laws. Although the Decree holds a lower legal status than a code or law in Vietnam's statutory hierarchy, it represents a significant step towards robust data protection. On 24 September 2024, the Vietnamese government released the first draft of a comprehensive personal data

protection law for public feedback. Subsequently, in March 2025, an updated version of the draft Law on Personal Data Protection (draft Law) was unofficially released. This draft Law introduces more detailed provisions and requirements compared to the current Decree and is expected to take effect on 1 January 2026.

The Cybersecurity and High-Tech Crime Prevention Department within the Ministry of Public Security (MPS) is responsible for enforcing the Decree, which took effect on 1 July 2023. Organizations were given two months to adjust their operations for compliance. By introducing alternative legal bases in the Decree, Vietnam aligns more closely with international standards.

Vietnam's data protection regulations include a clear definition of sensitive personal data and associated stricter processing requirements. While the range of sanctions at present is not as severe as in some other jurisdictions, it still provides a strong incentive for compliance.

1. ***The Decree recognizes six legal bases for processing personal data, with consent being the primary basis.***

   Data subjects' consent applies to all activities in the processing of personal data unless an alternative legal basis or exception applies. This encompasses a wide range of activities, including the collection, storage, analysis, disclosure, and deletion of personal data.

   Consent from the data subject is also one of the requirements for the transfer of personal data out of Vietnam, highlighting the critical role of consent in both domestic and international data processing activities.

1.1. **Conditions for "valid consent" under the Decree require that data subjects voluntarily and clearly understand certain aspects of processing.** Article 11 outlines these conditions, emphasizing that consent must be explicit, documented, and verifiable. It cannot be inferred from silence or non-response and can be partial or conditional, granted for specific purposes.

1.2. **Transparency and notice are integral to securing valid consent.** Article 13 mandates that data subjects must be fully informed before their personal data is processed, including details of potential risks of processing. Data subjects also retain the right to withdraw their consent at any time.

1.3. **Before processing sensitive personal data, data subjects must be informed of its sensitive nature.** The Decree defines "sensitive personal data" as personal data associated with an individual's privacy, the compromise of which would directly impact their legitimate rights and interests. It includes a non-exhaustive list of specific types of personal data considered sensitive.

1.4. **The Decree requires the consent of both parents (or guardians) and children aged seven or older for the processing of children's personal data.** It also requires all parties involved to verify the child's age before proceeding with any processing. In contrast, the DPDPA and the GDPR require parent or guardian

consent for minors under eighteen and sixteen, respectively, highlighting notable jurisdictional differences.

1.5. **Consent is a necessary but not sole requirement for transferring personal data out of Vietnam.** Specifically, before transferring personal data of Vietnamese citizens abroad, a highly detailed impact assessment dossier must be prepared. This documentation includes obtaining consent from the data subject.

2. ***The Decree allows for the processing of personal data without consent in certain situations.***

Article 17 of the Decree provides circumstances under which personal data may be processed without the consent of the data subject, emphasizing urgent situations and legal obligations:

- To fulfill the contractual obligations of the data subject with relevant entities.
- To protect the life and health of the data subject or others.
- Where the personal data is publicly disclosed in accordance with the law (Việc công khai dữ liệu cá nhân theo quy định của luật).
- For emergencies related to national defense, security, public order, major disasters, or dangerous epidemics.
- To serve state agency activities as prescribed by specialized laws.

The Decree shares common ground with the GDPR by permitting data processing for contractual obligations. However, it primarily prioritizes national interests and specific emergency scenarios–in particular, national security, public order, and terrorism. While this specificity offers clarity, the Decree lacks provisions permitting the processing of personal data for "legitimate interests," which may limit flexibility in unforeseen circumstances.

3. ***The Decree's approach to legal bases for data processing is complemented by its enforcement provision, seen in Article 4.***

This Article establishes that violations of personal data protection regulations can lead to disciplinary action, administrative sanctions, or even criminal prosecution, depending on the severity of the violation. This enforcement mechanism adds weight to the legal bases outlined in the Decree, creating a balance between allowing necessary data processing and ensuring accountability. While Article 17 provides specific scenarios for processing without consent, Article 4 serves as a deterrent against misuse or overreach.

In addition, while this Decree does not specify fines, on 2 May 2024, Vietnam's Ministry of Justice released documents evaluating a draft decree (Draft Penalty Decree) on penalties for data protection and

cybersecurity violations. These documents include a report from the MPS recommending the Draft Penalty Decree's adoption and a summary of public consultation responses since 2021. Under the proposed Draft Penalty Decree, organizations breaching data localization requirements outlined in Vietnam's existing cybersecurity decree may face fines of up to 100 million dong (approximately 4,000 USD). For repeated violations or significant personal data breaches, more severe penalties, such as fines of up to 5% of an organization's previous year's revenue in Vietnam, may be imposed.

It also remains to be seen whether the GDPR-style specific fine structure approach is adopted by Vietnam in its upcoming comprehensive law.

## Indonesia

On 20 September 2022, Indonesia's House of Representatives passed the Personal Data Protection Bill (PDP Bill). With Presidential assent on 17 October 2022, it was officially enacted as the Personal Data Protection Law (PDPL), Law No. 27 of 2022, effective immediately. The PDPL allows a two-year transition period, requiring organizations to comply with its provisions by October 2024. The PDPL provides a comprehensive framework for data protection in Indonesia, and efforts are underway to prepare implementing regulations to detail its specific provisions.

Furthermore, Article 28G(1) of the Indonesian Constitution provides general guidance on protecting citizens' data, providing the right of individuals to protection of their personal selves, families, respect, dignity, and possessions, reinforcing the legal framework provided by the PDPL.

Prior to the PDPL, Indonesia's data protection measures were dispersed across over thirty different laws and regulations. Various sector-specific, issue-specific, and nature-specific regulations addressed data protection and will remain valid as long as they do not contradict the PDPL. The new law aligns with international standards like the GDPR, outlining specific rights for individuals and responsibilities for data processors.

1. ***The PDPL resembles the GDPR's six legal bases for processing personal data.***

   Like the GDPR, the PDPL recognizes consent, along with alternatives to consent — contractual necessity, legal obligations, vital interests, public interest, and legitimate interests — as valid grounds for data processing.

   The legitimate interests basis in the PDPL maintains the core principle of balancing the controller's interests against the rights of the data subject. However, while the GDPR explicitly states that these interests can be overridden by the data subject's rights and freedoms, with specific mention of children's protection, the PDPL is slightly less detailed in this regard. For vital interests, the PDPL refers only to the data subject's interests, whereas the GDPR extends protection to other natural persons as well.

***1.1.*** **To process personal data under the "consent" legal basis, the data subject must give explicit and valid *consent* for one or more specific purposes.** Detailed conditions for obtaining and processing consent are described in Articles 21 to 25 of the PDPL. The data subject has the right to withdraw consent, and the controller is required to cease processing within seventy-two hours of the withdrawal of consent.

***1.2.*** The law requires that consent for **processing personal data of children** must be obtained from their parents or legal guardians, although it does not specify an age threshold for children.

***1.3.*** **The PDPL allows for cross-border data transfers based on consent when other legal bases are not feasible.** It stipulates that personal data can be transferred to entities outside Indonesia under specific conditions: specifically, the receiving entity must guarantee a comparable level of personal data protection and implement adequate and binding data protection measures. If these conditions cannot be ensured, explicit consent from the data subject is required for such transfers to proceed.

***2.*** ***The range of penalties outlined in the PDPL serve to deter unauthorized collection, disclosure, or use of personal data.***

Articles 67 to 73 reinforce the need for organizations to ensure they have a valid legal basis for all data processing activities. The law introduces more severe penalties for violations resulting in harm or death to the data subject, aligning with the inclusion of "vital interests" as a legitimate basis for processing. Penalties also escalate based on the severity of the violation, reflecting the PDPL's balanced approach in weighing diverse interests, similar to the consideration required under the "legitimate interests" basis. The inclusion of penalties for creating false personal data or falsifying data aligns with the public interest basis for processing.

The PDPL outlines both administrative and criminal sanctions for violations related to personal data protection. Criminal sanctions include imprisonment and fines, while corporate accountability may lead to higher fines and additional penalties like profit confiscation or business suspension. Administrative measures include warnings, data processing suspensions, data deletion, and fines. However, the full implementation and efficacy of these measures will depend on the yet-to-be-established supervisory authority.

## The Philippines

In the Philippines, the Data Privacy Act of 2012 (Republic Act No. 10173) (DPA) serves as the cornerstone of personal data protection, officially coming into full effect in September 2017. This legislation established the National Privacy Commission (NPC), an independent entity entrusted with administering and implementing the DPA. Since its establishment, the NPC has been actively issuing guidance on the DPA. One of its first actions was

to release the Implementing Rules and Regulations (IRR) for the DPA in September 2016, providing clarity on how the DPA's requirements are applied in practice.

Central to the DPA is the concept of consent, a fundamental principle governing the processing of personal data. While the Philippines has not introduced new legislation, the NPC has issued significant clarifications:

- On 7 November 2023, the NPC issued Circular No. 2023-04–"Guidelines on Consent" (Consent Circular), providing substantial clarification and guidance on using consent as a lawful basis for processing personal data.
- On 13 December 2023, the NPC issued Circular No. 2023-07–"Guidelines on Legitimate Interest," (LI Circular), clarifying the use of legitimate interest as a lawful basis for processing personal data under the DPA.

Notably, although titled "guidelines," the circulars are binding. Section 23 and Section 14 of the Consent Circular and LI Circular respectively stipulate that non-compliance can lead to criminal, civil, and administrative penalties under the DPA.

The focus on user-friendly consent processes and the acknowledgment of "consent fatigue" address modern data protection challenges. Clarifications on legitimate interests provide guidance for businesses using this legal basis. The Circulars do not change the fundamental legal framework but impact the interpretation and application of existing law.

1. ***The Consent Circular outlines criteria for obtaining consent under the DPA, emphasizing it must be provided voluntarily, without any form of coercion***.

   The DPA defines "consent of the data subject" as a "freely" given, "specific," and "informed" "indication of will" by the data subject for the collection and processing of their personal information; and that it must be "evidenced by written, electronic or recorded means." The Consent Circular elaborates on quoted elements of the definition by providing that consent should not be coerced, should carry no adverse consequences, and must be explicitly linked to declared purposes. It should also provide enough information to facilitate informed decision-making and must be signified through clear affirmative actions.

   Specifically for sensitive personal information, consent needs to be "specific to the purpose" and secured before any data collection occurs. For non-sensitive information, consent can be obtained either before or immediately after collection. Furthermore, a lawful representative or authorized agent can give consent on behalf of the data subject if necessary.

1.1. **Valid consent requires that data subjects be provided with concise information at the time of obtaining consent** – about the nature, purpose, scope, associated risks, safeguards, and their rights, supplemented by detailed information through a layered privacy notice. Examples of notices include: notifications

displayed during application installation, contextual prompts, and just-in-time notices prior to data processing.

1.2. **The Consent Circular addresses the issue of "consent fatigue"**—the phenomenon where data subjects are overwhelmed by frequent and complex consent forms, leading to improperly given consent—by advising Personal Information Controllers (PICs) to establish a lawful basis for processing data before collection. It cautions against unnecessary consent requests and encourages PICs to determine if an alternative lawful basis under the DPA suffices, thereby minimizing the risk of consent fatigue and enhancing the integrity of consent mechanisms.

1.3. **While the DPA is silent on the withdrawal of consent, the IRRs indicate that consent can be withdrawn, and the Consent Circular provides further details.** Section 13 of the Consent Circular specifies that data subjects have the right to withdraw their consent at any time without cost, unless lawfully restricted. One of the key aspects of withdrawal (common with DPDPA) is to ensure that withdrawing consent is as simple as giving it, if not simpler, as well as establishing straightforward procedures for data subjects to request data erasure.

1.4. The Consent Circular also **prohibits "bundled consent" practices** — ensuring that consent is specific and not assumed from the presence of personal data on public platforms.

2. ***The DPA permits processing personal data without consent if necessary for "legitimate interests," provided these interests do not override the data subject's fundamental rights and freedoms.***

The DPA acknowledges alternatives to consent, including contractual necessity, legal obligations, vital interests, national emergency, and legitimate interests, as valid grounds for processing data.

The NPC issued the LI Circular clarifying the use of legitimate interest as a lawful basis for processing personal data under the DPA.

2.1. **What is "legitimate interest"?** It describes "legitimate interest" as any actual and real benefit or gain that a PIC or third party may have from processing specific personal information. At its core, the concept of legitimate interest allows PICs and authorized third parties to process personal data when they have a real, justifiable need.

However, this is not a blank check—the LI Circular emphasizes that this basis cannot be used for sensitive or privileged information, and the interests of the organization must be carefully balanced against the privacy rights of individuals.

2.2. **Organizations must conduct a legitimate interest assessment before processing personal data.** The Circular introduces a three-part test that PICs must conduct:

- First, they must clearly establish their legitimate interest, defining a specific purpose that is both lawful and transparent to the individuals involved.
- Second, they need to prove that their chosen method of processing is necessary and proportional to achieve that purpose.
- Finally, and perhaps most crucially, PICs must perform a balancing test. This involves weighing their interests against the potential impact on individuals' rights and freedoms. They need to consider factors like the effects of the processing, any safeguards in place, and whether individuals would reasonably expect their data to be used in this way.

PICs are required to keep detailed records of their assessments, which may be reviewed by the NPC during investigations or compliance checks. This encourages accountability and allows organizations to demonstrate their decision-making process. The Circular encourages sectors to develop their own specific legitimate interest frameworks, tailored to common practices within their field. While the guidelines are comprehensive, they also recognize that different industries may have unique needs.

3. ***The penalties provisions in both Consent and Legitimate Interests Circulars emphasize that violations can result in criminal, civil, and administrative sanctions.***

The penalties provision under Section 23 of the Consent Circular emphasizes the critical importance of proper consent management within the Philippine data protection law. The detailed guidelines and strict requirements set forth in the Consent Circular underscore the significance of consent as a legal basis. The comprehensive penalty structure serves as a strong deterrent, motivating organizations to implement the circular's guidelines thoroughly. By referencing the DPA, its IRRs, and other Commission directives, the Circulars position themselves within the broader regulatory framework.

## South Korea

South Korea's primary personal data protection law is the Personal Information Protection Act (PIPA), which has been in effect since 30 September 2011. This law is supported by an enforcement decree, various sector-specific laws (such as those in the credit, telecommunications, and insurance sectors), and guidelines from the Personal Information Protection Commission (PIPC), the country's data protection regulator. The most significant amendments to PIPA were in 2020 and 2023.

Since its enactment in 2011, PIPA has established various legal bases for processing personal data, including both consent and alternatives to consent that broadly align with major international data protection frameworks, such as the GDPR. Compared to the GDPR, PIPA imposes stricter conditions for relying on alternatives to consent,

however, amendments to the PIPA, which took effect in 2023, have lowered the threshold for two specific bases, bringing PIPA more in line with GDPR standards (see below).

In recent years, South Korea has taken significant steps to enhance its data protection framework, focusing on improving transparency in consent processes and enhancing its legal bases for data processing.

1. ***In 2022, PIPC issued guidelines providing greater clarity on consent requirements under the PIPA.***

   On 3 March 2022, the PIPC introduced two sets of guidelines (Guidelines)–(1) the "Easy-to-Understand Manual on Consent for Personal Data Processing" and (2) "Guidelines for Writing Privacy Policies"–which aim to make the process of obtaining consent and understanding personal data processing more accessible to data subjects.

   While the Guidelines are not technically binding, they do provide a framework that will help organizations comply with the PIPA and avoid administrative sanctions.

1.1. **The Guidelines aim to prevent situations where individuals give consent without fully understanding, often termed "read-only consent."**

   The PIPC's Guidelines aim to increase transparency by outlining comprehensive instructions that emphasize transparency, data minimization, and user empowerment throughout the data processing lifecycle.

1.2. **The principles of minimization and transparency should be followed when obtaining consent.**

   The Guidelines establish four principles that data controllers should follow when obtaining data subjects' consent for the processing of their personal data. These include:

   - Limiting the amount of personal data requested to the minimum necessary.
   - Clearly informing the data subjects about how and by whom their data will be handled.
   - Using straightforward language to confirm that data subjects understand and agree to specific data uses.
   - Ensuring that data subjects freely consent without facing penalties for refusal.

1.3. **The Guidelines suggest that organizations use graphics in their privacy notices to inform data subjects about various data processing activities.** They recommend including key information on data transfers, children's consent, emergency data processing, and safety measures, using symbols and infographics for clarity.

1.4. **Specific instructions are provided for writing personal information processing policies tailored to various industries**, including hospitals, academies, travel agencies, public institutions, and online

platforms. These instructions cover essential details such as the purpose of data processing, retention periods, destruction procedures, rights of data subjects, safety measures, and the roles of data protection officers.

1.5. **The Guidelines also outline necessary information that must be provided to data subjects before their consent is considered valid.** For instance, data controllers must inform data subjects that their use of a given service will not be restricted if they refuse to consent to processing of their personal data.

*2.* ***In early 2023, South Korea's National Assembly passed significant amendments to the PIPA lowering the threshold for relying on certain alternatives to consent.***

On 15 September 2023, a majority of the amendments to the PIPA and its Enforcement Decree, which were promulgated in March 2023, came into force. Among other things, these amendments established additional legal bases for cross-border data transfers and lowered the threshold for relying on certain alternative bases to consent under the PIPA. The 2023 amendments align the PIPA's legal bases for processing personal data even more closely with those in the GDPR.

2.1. **The amendments in 2023 unified the obligations for both online and offline businesses under the PIPA, resulting in a more consistent regulatory framework.** This imposed additional data protection responsibilities on offline businesses, which were previously only required of online businesses, and provided more relaxed standards for online businesses. As a result of the 2023 amendments, all provisions of the PIPA, including legal bases for collecting and using personal data, now apply equally to both online and offline businesses.

2.2. **The 2023 amendments, in particular to Article 15, relax the conditions under which data can be collected and used without consent.**

a. **Following the amendments, data controllers in South Korea may collect and use personal data without consent if the collection or use is "necessary" for the performance or execution of a contract.** This change lowers the threshold from the earlier provision, which required the processing to be "inevitably necessary" for these purposes, providing greater flexibility for data controllers.

b. **The amended provisions also lower the threshold for collecting or using personal data without consent in situations of imminent danger to life, bodily, or property.** Specifically, they remove the earlier provision's requirement for data controllers to demonstrate that consent could not be obtained before they can collect or use personal data for this purpose. This broadens the scope for data collection or use in emergency situations, making it easier to act swiftly without needing consent, even if it is possible to obtain it.

c. The amendments also introduce new provisions that allow the collection and use of personal data without consent when **urgently necessary for public safety, security, and health**.

These changes mark a significant shift from South Korea's previous two-decade-old system of mandatory consent. While the benefits are clear on paper, such as shifting more of the burden of managing data to businesses and opening up more opportunities for companies to innovate using data, it will take time for companies to adjust to the new paradigm. Some companies are taking a wait-and-see approach before implementing changes, and are hoping that forthcoming guidelines from the PIPC in December 2024 will help clarify uncertainties that companies face.

2.3. **The 2023 amendments expand the legal bases for cross-border data transfers.**

Prior to the 2023 amendments, data controllers could only transfer personal data out of South Korea if they obtained the data subject's consent or if the transfer was otherwise permissible under specific laws, treaties, or international agreements. The 2023 amendments facilitate cross-border data transfers by introducing new legal bases for transferring personal data out of South Korea without data subjects' consent. These new bases allow for such transfers if:

a. **it is necessary for the execution or performance of a contract with the data subject.** The data subject must also be informed of the transfer, or it must be disclosed in the data controller's privacy policies.

b. **the overseas recipient has received data protection certification from the PIPC** and has taken necessary data protection measures.

c. **the PIPC recognizes that the destination country or international organization provides an adequate level of data protection** to the transferred data, compared with the protection that it would receive under the PIPA.

d. Notably, unlike the GDPR and similar data protection laws, the PIPA does not provide transfer mechanisms based on standard contractual clauses or binding corporate rules.

## Malaysia

In Malaysia, the primary framework for data protection is established by the Personal Data Protection Act 2010 (PDPA), which is enforced by the Personal Data Protection Department (PDPD). This legislation is complemented by various sector-specific laws that govern the disclosure of personal data by entities such as financial service providers and medical practitioners. On 16 July 2024, the lower house of Malaysia's bicameral Parliament, the House of Representatives (Dewan Rakyat), passed the Personal Data Protection (Amendment) Bill 2024 (PDP Amendment Bill) following its second and third readings. This milestone came after Malaysia's Digital Minister, Gobind Singh Deo, introduced the PDP Amendment Bill for its first reading on 10 July 2024. On 17 October 2024,

the Personal Data Protection (Amendment) Act 2024 (PDP Amendment Act) was published in Malaysia's Federal Gazette after receiving Royal Assent on 9 October 2024. This PDP Amendment Act does not modify the fundamental legal bases for data processing or the nuances of obtaining consent, but introduces several significant provisions.

1. **The PDPA emphasizes the importance of consent as the main legal basis for the lawful processing of personal data**. It stipulates that data controllers must obtain consent from data subjects to collect, use, and disclose personal data, although there are exceptions for scenarios such as:

    a. To perform a contract to which the data subject is a party.

    b. To take steps at the request of the data subject while negotiating a contract.

    c. To comply with any legal obligation to which the data controller is the subject.

    d. To protect the vital interests of the data subject.

    e. For the administration of justice.

    f. For the exercise of any functions conferred on any person by or under any law.

    Notably, **PDPA does not include the concept of "legitimate interests"** as found in the GDPR, relying instead on a consent-based model as outlined in the general principle–Section 6 of the PDPA.

    **For sensitive personal data, the PDPA mandates explicit consent unless certain exceptions apply**, such as seeking legal advice or for protection of vital interests where consent cannot be obtained.

2. **The PDPA does not specify the exact forms that consent can take, but sub-regulations state that consent must be capable of being recorded and maintained by the data controller.** Furthermore, consent forms should be designed to distinctly separate specific consent from other content included within the same form. In addition, data controllers are required to ensure transparency by clearly detailing their data processing activities within their privacy policies, a requirement that mirrors the transparency obligations under the GDPR.

3. **In a significant development on 17 October 2024, the PDP Amendment Act was published in Malaysia's Federal Gazette after receiving Royal Assent.** This PDP Amendment Act does not alter the legal bases for data processing or clarify the nuances of obtaining consent. Instead, it introduces several key provisions, including:

    a. New definitions for key terms, such as "personal data breach" and "biometric data."

    b. The introduction of a right to data portability.

c. The mandatory appointment of data protection officers and to notify the PDPD of the appointment.

d. The introduction of stricter data breach notification requirements, with significant penalties for non-compliance, including potential fines of up to MYR 250,000 (approximately US$53,540) or imprisonment up to two years, or both.

e. Revision of the approach to cross-border data transfers, replacing the existing whitelist (which has not been implemented to date) with new provisions allowing data controllers to transfer personal data outside Malaysia if the destination has substantially similar laws to the PDPA or ensures an adequate level of protection equivalent to that provided by the PDPA.

f. Requirement for data processors to comply with the PDPA's security principle, with increased penalties of up to MYR 1 million (approximately US$212,530) and imprisonment of three years for non-compliance.

## Australia

In Australia, data protection is primarily governed by the Privacy Act 1988 (Privacy Act), which was passed in 1988. The 2010 amendments to the Privacy Act established the Office of the Australian Privacy Commissioner (OAIC), which serves as Australia's primary regulatory body for privacy protection and oversees compliance with the Privacy Act. This legislation incorporates the Australian Privacy Principles (APPs) and is complemented by sector-specific regulations governing data protection across different industries. Over the past three decades, the Privacy Act has undergone several significant amendments. In December 2024, the Australian Parliament passed the Privacy and Other Legislation Amendment Bill 2024 (Amendment Bill), marking the most substantial reform to Australia's privacy framework since 2014. While the Amendment Bill introduces significant changes to its privacy laws, it does not alter the fundamental legal bases for data processing or consent requirements.

1. ***The Privacy Act establishes distinct requirements for consent depending on the type of personal information and the processing activity.***

   The APPs do not mandate consent for collecting personal information directly from an individual–it is generally sufficient if the information is necessary for an organization's function or activity and is collected lawfully and fairly, and if reasonable steps are taken to notify the individual as required by APP 5.

   However, consent is mandatory for using or disclosing personal information for secondary purposes—those beyond the reasons for its initial collection as outlined in APP 6.1. For sensitive personal

information, explicit consent is required for both its collection (APP 3.3) and its use or disclosure (APP 6.1), unless specific exceptions are applicable.

1.1. **Consent serves as an exception that allows certain acts, which would otherwise be prohibited under the APPs, including:**

- Collection of personal information from sources other than the data subject.
- Use or disclosure of personal information for purposes different from those for which it was originally collected.
- Use of personal information for direct marketing purposes.
- Cross-border transfer of personal information without taking reasonable steps to ensure the overseas recipient does not breach the APPs.

2. ***On 10 December 2024, the Amendment Bill received Royal Assent, becoming the Privacy and Other Legislation Amendment Act 2024 (Amendment Act).***

The Amendment Bill was introduced to the Australian House of Representatives on 12 September 2024, following a multi-year consultation process, and it was passed by the Australian Senate on 29 November 2024. This marks the most substantial reform to Australia's privacy framework since 2014.

2.1. **The Amendment Act does not alter the fundamental legal bases for data processing or the requirements for obtaining consent.** However, it does introduce several significant provisions, including:

a. A requirement for the OAIC to develop a Children's Online Privacy Code within two years.

b. Expanded investigatory and monitoring powers for the Information Commissioner, including the power to conduct public inquiries.

c. A statutory tort for serious privacy breaches.

d. Increased transparency requirements for automated decisions that could reasonably be expected to significantly affect individuals' rights and interests.

e. A tiered civil penalty regime allows the OAIC to tailor penalties based on the severity of the infringement.

f. Additional enforcement powers for courts in civil penalty proceedings, including ordering corrective actions, awarding damages, and requiring entities to publish statements acknowledging infringements.

g. Prohibition of doxxing, with severe penalties for malicious use of personal data.

3. ***In October 2024, the OAIC released significant guidance explaining how the Privacy Act and the APPs apply in the AI context.***

On 21 October 2024, the OAIC released two significant sets of guidelines addressing privacy in AI: (1) the "Guidance on privacy and developing and training generative AI models" (AI Development Guidelines), and (2) the "Guidance on privacy and the use of commercially available AI products" (AI Product Guidelines) (collectively, "OAIC Guidelines").

The OAIC Guidelines establish clear parameters for the legal basis of processing personal data in AI contexts. Notably, the OAIC Guidelines highlight the conditions for lawfully collecting publicly available personal information for training generative AI models and provide privacy guidance for organizations using AI systems that process personal information.

It sets standards under the Privacy Act and its 13 APPs, with a particular focus on accuracy, transparency, and increased oversight of the collection of personal information and its secondary use.

3.1. **The AI Development Guidelines target developers of AI systems** and focus on privacy considerations that arise when training generative AI models on datasets containing personal information. Key points include:

a. Publicly available data cannot be automatically used for AI training without meeting privacy obligations.

b. APP 3 requires developers to only collect personal information that is reasonably necessary, using lawful and fair means and avoiding covert methods like web scraping unless justified. The AI Development Guidelines elaborate on what constitutes "fair" means.

c. Sensitive information generally requires explicit consent for collection (APP 3) or use (APP 6). Developers must ensure consent is obtained before processing sensitive data, including images or recordings, in AI models.

d. When using personal information for AI-related purposes that were not the primary reason for collection, APP 6 requires developers to ensure that the secondary use is reasonably expected by the individual or that consent is obtained. When secondary AI use cannot be clearly justified, developers should obtain consent or provide meaningful opt-out options to avoid regulatory issues.

e. Generative AI systems are probabilistic and can produce inaccurate results, raising concerns under APP 10. Developers must take reasonable steps to ensure the accuracy of personal data used, including employing quality datasets, conducting testing, and implementing safeguards based on risk levels.

3.2. **The AI Product Guidelines address organizations deploying AI systems that process personal information**. Notable aspects include:

a. The generation or inference of personal information by AI models is considered data collection and must comply with APP 3. Organizations are required to ensure that the generation of personal information by AI is reasonably necessary and is only done by lawful and fair means.

b. Personal information input into AI systems can only be used for its primary collection purpose unless consent exists or secondary use meets reasonable expectations (APP 6).

c. Organizations should avoid entering personal and especially sensitive information into publicly available AI tools due to significant privacy risks.

## Conclusion

The APAC region has recently witnessed significant developments in data protection, with new laws and guidelines in India, Vietnam, Indonesia, the Philippines, South Korea, and Malaysia. However, it is crucial to recognize the distinct nuances in each country's approach. For instance, India, Vietnam, and Indonesia do not explicitly recognize "legitimate interests" as a legal basis for processing personal data, while the Philippines has provided dedicated guidelines clarifying its use under their Data Privacy Act.

This diversity in approaches, while reflecting local contexts, highlights the ongoing challenge of achieving regional harmonization. The incorporation of the GDPR-inspired elements alongside stricter requirements for sensitive data and children's information indicates a convergence towards global standards, but with significant regional variations.

As these frameworks transition from legislation to implementation, monitoring their practical impact and enforcement will be crucial. The effectiveness of novel concepts and regulatory interpretations of alternative legal bases will significantly influence data protection's future in the region. Looking ahead, the APAC region will continue to evolve dynamically. The interplay between new laws, existing sector-specific regulations, and global standards will be vital in developing a coherent yet flexible approach, ensuring these frameworks can effectively protect individual rights and foster innovation amidst diverse national approaches and rapid technological advancements.


Washington, DC | Brussels | Singapore | Tel Aviv

info@fpf.org

FPF.org