NOVEMBER 2022

BALANCING ORGANIZATIONAL ACCOUNTABILITY AND PRIVACY SELF-MANAGEMENT IN ASIA-PACIFIC

A comparative analysis of legal bases for processing of personal data across data protection laws in Asia-Pacific

FUTURE OF PRIVACY FORUM

ASIAN BUSINESS LAW INSTITUTE

AUTHOR

Dominic Paulger
Future of Privacy Forum (APAC)

ACKNOWLEDGMENTS

ABLI and FPF gratefully acknowledge the contributions of:

- Dr Clarisse Girot, OECD (Paris)
- Anna Johnston, Salinger Privacy (Australia)
- Kemeng Cai, Han Kun Law Offices (China)
- Mark Parsons, Hogan Lovells (Hong Kong SAR)
- Malavika Raghavan, Dvara Research (India)
- Danny Kobrata and Bhredipta Socarana, K&K Advocates (Indonesia)
- Professor Masahiro Sogabe, Professor Yuko Nishitani, and Ryoya Shibaike, Kyoto University (Japan)
- Takeshige Sugimoto, S&K Brussels (Japan)
- Graça Saraiva, Sands China (Macau SAR)
- Deepak Pillai, Christopher & Lee Ong (Malaysia)
- Daimhin Warner, Simply Privacy (New Zealand)
- JJ Disini and Ofelia Leaño, Disini & Disini (The Philippines)
- Lim Chong Kin and David Alfred, Drew & Napier (Singapore)
- Kwang Bae Park, Lee & Ko (South Korea)
- Thitirat Thipsamritkul, Thammasat University (Thailand)
- Auradee Wongsaroj (Thailand)
- Tong Khanh Linh, Institute for Policy Studies and Media Development (Vietnam)
- Waewpen Piemwichai, Tilleke & Gibbins (Vietnam)

This Review benefitted from contributions and editing support from Catherine Shen (ABLI), Dr. Gabriela Zanfir-Fortuna (FPF), Hunter Dorwart (FPF), Lee Matheson (FPF), Isabella Perera (FPF), and Josh Lee Kok Thong (FPF).

DISCLAIMER

This Comparative Review ("**Review**") provides a detailed comparison of the legal bases for processing personal data in the data protection laws and regulations of 14 jurisdictions in Asia-Pacific, namely:

- Australia;
- China;
- Hong Kong Special Administrative Region of the People's Republic of China ("**Hong Kong SAR**");
- India;
- Indonesia;
- Japan;
- Macau Special Administrative Region of the People's Republic of China ("**Macau SAR**")
- Malaysia;
- New Zealand;
- The Philippines;
- Singapore;
- South Korea;
- Thailand; and
- Vietnam

Despite differences in the regulatory structures and underlying philosophies of each jurisdiction's data protection framework, this Review identifies connecting points between these frameworks to aid efforts by lawmakers, governments, and data protection regulators to promote legal convergence or interoperability in the Asia-Pacific region.

ABOUT THE ASIAN BUSINESS LAW INSTITUTE

The Asian Business Law Institute ("**ABLI**") is a neutral, non-profit permanent institute based in Singapore dedicated to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

ABLI seeks to address key problems resulting from legal diversity in Asia identified by stakeholders in the public and private sectors.

ABLI's long-term strategic direction is set by its Board of Governors, chaired by the Honourable the Chief Justice Sundaresh Menon of the Supreme Court of Singapore. The Board of Governors comprises representatives of the judiciaries of Australia, China, Singapore, and India, as well as other internationally renowned legal experts.

Since 2017, ABLI has undertaken a multi-stakeholder project focusing on the regulation of international data transfers in 14 Asian jurisdictions, in collaboration with a wide range of stakeholders including law practitioners, industry representatives, and academics, with input from data protection and privacy commissions and governments of the region which are currently working on, or reviewing, their respective data protection frameworks.

ABOUT THE FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a global non-profit organization that brings together academics, civil society, government officials, and industry to evaluate the societal, policy, and legal implications of data use, identify the risks, and develop appropriate protections. FPF has offices in Washington D.C., Brussels, Singapore, and Tel Aviv. Learn more at **fpf.org**.

TABLE OF CONTENTS

Why this Review? 1

Need for Convergence or Interoperability in a Period of Intensive Law Reform 3

Comparative Analysis of Data Protection Laws in Asia-Pacific 5

Legal Bases for Processing Personal Data 7

Legitimate Interests 56

Collective Benefits of Legal Certainty and Convergence 63

Rebalancing Consent and Privacy Accountability in Asia-Pacific: A Roadmap 64

Recommendations 75

Endnotes 85

ABLI Data Privacy Project

In 2016, ABLI initiated a Data Privacy Project ("**Project**")[1] to provide a framework for dialogue, research, and other activities with the aims of increasing legal certainty, accessibility, and availability of laws and regulations relating to data protection and privacy, facilitating cross-border compliance efforts by organizations, and promoting legal convergence to ensure a consistently high level of data protection for individuals across the Asia-Pacific region.

The work themes addressed in the Project are selected based on the suggestions and needs of a wide network of public and private stakeholders in the region, including data protection regulators, privacy professionals, legal practitioners, academics, think tanks, etc.

A precedent: "Transferring Personal Data in Asia: A path to legal certainty and regional convergence"

The first line of work in the Project focused on cross-border data transfer regulations in Asia-Pacific. This work demonstrated the challenges that arise from divergence in laws, regulations, and other frameworks across the region, and the negative impact of such divergence on private stakeholders that operate across borders, data subjects, and regulators.

This work also led to several publications, including a landmark paper – ***"Transferring Personal Data in Asia: A path to legal certainty and regional convergence"*** (ABLI, May 2020)[2] – that provides a detailed comparative analysis of data transfer regulations in Asia-Pacific and sets out proposals for regional stakeholders to promote legal certainty and greater consistency in requirements for cross-border transfer of personal data.

Notice and choice, consent, and alternative legal bases for processing personal data in Asian data protection laws

ABLI's network of stakeholders has consistently given feedback that the areas most in need of regulatory coherence in Asia-Pacific are the implementation of consent requirements and the various alternatives and exceptions to those requirements. However, ABLI also received feedback that the culture of "compliance through consent" is so deeply ingrained in practice that no change can occur without resolute and coordinated action from regulators.

Therefore, in 2021, ABLI embarked on the second phase of the Project: identifying common ground in requirements for consent and other legal bases for processing personal data in regional laws and regulations which regulators, through coordinated efforts, could develop into a consistent set of norms for Asia-Pacific that would balance privacy accountability by organizations that process personal data and "privacy self-management"[3] by individual data subjects.

Cooperation between ABLI and FPF on the Data Privacy Project

Recognizing that personal data protection frameworks in Asia-Pacific are at a critical stage in their development as many jurisdictions in this region are in the process of adopting, implementing, or reforming their data protection laws and regulations, ABLI and FPF agreed in August 2021 to establish a platform to cooperate on joint research, publications, and events to promote convergence of data protection regulations and best privacy practices in Asia-Pacific.[4]

The first collaboration between ABLI and FPF took the form of an online seminar — "***Exploring Trends: From 'Consent-Centric' Frameworks to Responsible Data Practices and Privacy Accountability in Asia Pacific***"[5] — which was co-hosted by Singapore's Personal Data Protection Commission ("**PDPC**") during Singapore's Personal Data Protection Week in September 2021. This event highlighted the limits of the consent-based approach to data protection both in Asia-Pacific and globally, and the value in developing alternative legal bases for processing personal data, such as "legitimate interests."

Building on the findings from this joint event, ABLI and FPF undertook a comprehensive assessment of the role and position of notice, consent, and other legal bases for processing personal data in the laws and regulations of 14 jurisdictions in Asia-Pacific.

This assessment led to the publication of 14 detailed jurisdiction reports under the "***ABLI-FPF Series on Convergence of Data Protection and Privacy Laws in APAC.***" These reports drew from the professional knowledge, experience, and opinions of a wide range of expert contributors from across Asia-Pacific and provide a detailed overview of relevant laws and regulations in each jurisdiction on:

- consent requirements for processing personal data;
- legal bases for processing personal data without consent which involve an impact assessment (e.g., legitimate interests); and
- statutory bases for processing personal data without consent and exceptions or derogations from consent requirements in general and sector-specific laws and regulations.

The findings of these reports have informed this Review, which provides lawmakers, governments, and regulators in Asia-Pacific who are currently drafting, reviewing, or implementing their respective data protection laws with a comparative overview and analysis of legal bases for processing personal data in the data protection frameworks of their regional partners and neighbors.

NEED FOR CONVERGENCE OR INTEROPERABILITY IN A PERIOD OF INTENSIVE LAW REFORM*

In recent years, there has been a massive increase in data protection laws in Asia-Pacific. Most jurisdictions now have comprehensive data protection legislation or have released draft legislation and are on track to enacting comprehensive data protection laws in the near future. For example:

- **Vietnam** is working on comprehensive new data protection legislation, which is expected to be passed in 2022.
- After withdrawing its Data Protection Bill in August 2022, **India**'s Ministry of Electronics and IT released a new draft Digital Personal Data Protection Bill for public consultation on November 18, 2022.[6]

However, this diffusion of new data protection laws creates challenges for cross-border compliance, and all stakeholders who work in this space — primarily industry and legal practitioners, but also increasingly, the community of data protection regulators — acknowledge the need for greater consistency in regional data protection frameworks.

An obvious starting point for regional convergence or interoperability would be to focus on consent requirements, which (along with other legal bases for data processing) apply at the beginning of the data lifecycle.

Consent as a legal basis for processing is a common denominator across the data protection frameworks of the 14 jurisdictions in this Review. In fact, it is the only legal basis that is shared by all jurisdictions and that applies to all forms of personal data (whether sensitive or not) and all activities involving personal data.

Feedback from stakeholders suggests that organizations operating across borders often perceive consent as the "easiest" or "safest" way to achieve cross-border compliance. Further, even where individual jurisdictions do not strictly *require* consent for all forms of processing, organizations often seek consent anyway to "cover their bases," for example, because a consent form serves as proof that the business has complied with applicable notification requirements or because the business has implemented a cross-border compliance framework that was designed to comply with the requirements of more influential jurisdictions that recognize consent as a legal basis for processing of personal data. Further, "tick-the-box" compliance habits and reluctance to change the user experience may often lead organizations to fall back on consent.

However, efforts towards convergence should not ignore that over the past few years, many jurisdictions internationally have come to recognize the limitations of consent as a legal basis for processing personal data, especially in a digital environment. In particular, many jurisdictions in Asia-Pacific have been engaging in similar conversations around the need to reframe consent. For instance:

- In 2018, a Committee of Experts report on plans for a future data protection law in **India** described the operation of notice and consent on the Internet as "broken" and questioned whether consent alone could be an effective method for protecting personal data and preventing individual harm.[7]
- In 2019, **New Zealand**'s then-Privacy Commissioner declared in a much-cited blog post that click-to-consent mechanisms were "not good enough anymore" and called for consumers and businesses alike to rethink consent and move towards a "Privacy by Design" model.[8]

** Pages 3–4 co-authored by Dr. Clarisse Girot, Honorary Senior Fellow, ABLI, and Dominic Paulger, Policy Manager, FPF*

- In 2020, Singapore took the bold and unprecedented step in the region of restructuring its data protection law from a primarily consent-based framework to one permitting collection, use, and disclosure of personal data without consent in a wide range of situations, including "vital interests of individuals," "matters affecting the public," "legitimate interests," "business asset transactions," "business improvement purposes," and "research."[9]
- Since 2020, **Australia** has been undertaking a sweeping review of its Privacy Act, including consent requirements.[10]
- In February 2020, **Malaysia**'s Personal Data Protection Commissioner issued Public Consultation Paper No. 1/2020 which aims to collect feedback on the Commissioner's proposal to update the Personal Data Protection Act 2010. Among other things, the Commissioner is considering restructuring the Malaysian PDPA's consent provisions with a focus on the *"scope and application of consent through the personal data life cycle."*[11]
- **China**'s Personal Information Protection Law took effect in November 2021. Chinese regulators continue to issue further measures and guidance, including releasing several legislative documents seeking to restrain "bundled consent" over the past years, whether in baseline texts like the Personal Information Security Specification, or recently the Personal Information Protection Law and the Measures for the Supervision and Administration of Online Transactions.[12]
- **South Korea**'s Personal Information Protection Commission identified *"moving towards an easily understandable and clear Notice & Choice model"* as one of its main initiatives for 2021.[13]
- **New Zealand** is currently holding a public consultation on proposed reforms to notification requirements for collecting personal information under the Privacy Act 2020 with the aim of increasing transparency regarding the indirect collection of personal information.[14]

These developments represent a rare window of opportunity to clarify existing uncertainties and enhance the compatibility of regional data protection laws on these crucial issues. This Review therefore aims to initiate a regional dialogue on consent and alternatives to consent that could increase the accountability of organizations when they process personal data. In particular, this Review aims to identify available measures to rebalance protection of individuals from harm with recognition of the interests of organizations and broader society, such as developing a vibrant digital economy and preventing crime and fraud.

COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS IN ASIA-PACIFIC

This Review presents a comparison and analysis of the main data protection laws and relevant regulations governing processing personal data by private-sector entities in each of the 14 jurisdictions subject to this study. Where relevant, this Review also takes into account general guidelines on personal data protection issued by the data protection authority in each jurisdiction.

Use of unofficial translations. This Review has used up-to-date English-language versions of the relevant texts where data protection authorities have made such versions available. Where up-to-date English-language versions are unavailable, the Review has used unofficial English-language translations of the most up-to-date versions of relevant texts released by relevant authorities in the original languages.

Exclusion of sensitive personal data and sectoral laws, regulations, and guidelines. To avoid too wide a field of comparison, this Review has not considered categories of "sensitive" personal data (or equivalents) or sector-specific laws and regulations (e.g., in the telecommunications, banking, credit reporting, or health sectors).

Exclusion of practice and unofficial interpretations. The comparisons presented in this Review are also limited to textual analysis of the relevant laws, regulations, and guidelines. The Review has not focused on how the relevant provisions are interpreted and applied in practice, unless relevant authorities have issued interpretations in publicly-available guidance materials, such as guidelines and advisory opinions.

For further information on how relevant provisions are applied in practice and on the sectoral laws and regulations that impact personal data protection in the jurisdictions covered by this Project, please refer to the individual jurisdiction reports released as a complement to this Review.[15]

JURISDICTION	CODE	LAWS, REGULATIONS, AND GUIDELINES
Australia	**AU**	• Privacy Act 1988 ("**Privacy Act**"), especially the Australian Privacy Principles ("**APPs**")[16] • Australian Privacy Principles guidelines ("**APP Guidelines**")[17]
China	**CN**	• Personal Information Protection Law ("**PIPL**")[18] • Personal information security specification ("**Security Specification**")[19]
Hong Kong SAR	**HK**	• Personal Data (Privacy) Ordinance ("**PDPO**"), especially the Data Privacy Principles in Schedule 1 ("**DPPs**")[20]
India	**IN**	• Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**IT Rules**")[21] **Note:** The IT Rules apply only to certain types of personal data, termed "sensitive personal data or information" ("**SPDI**") • Draft Digital Personal Data Protection Bill, 2022 ("**Draft DPDPB**")[22] released for public consultation in November 2022
Indonesia	**ID**	• Personal Data Protection Law ("**PDPL**")[23]

JURISDICTION	CODE	LAWS, REGULATIONS, AND GUIDELINES
Japan	**JP**	• Act on the Protection of Personal Information ("**APPI**")[24] • Order for Enforcement of the Act on the Protection of Personal Information (Cabinet Order No. 507 of 2003) as amended in 2016 ("**Cabinet Order**")[25] • Guidelines on the Act on the Protection of Personal Information (General Rules) ("**APPI Guidelines**")[26] • Q&A regarding the "Act on the Protection of Personal Information ("**APPI Q&A**")[27]
Macau SAR	**MO**	• Personal Data Protection Act ("**PDPA**")[28]
Malaysia	**MY**	• Personal Data Protection Act ("**PDPA**")[29] • Personal Data Protection Regulations 2013[30]
New Zealand	**NZ**	• Privacy Act 2020 ("**Privacy Act**"), especially the Information Privacy Principles ("**IPPs**")[31]
The Philippines	**PH**	• Republic Act 10173 – Data Privacy Act of 2012 ("**DPA**")[32] • Implementing Rules and Regulations of the Data Privacy Act of 2012 ("**IRRs**")[33] • The National Privacy Commission's Advisory Opinions[34]
Singapore	**SG**	• Personal Data Protection Act ("**PDPA**")[35] • Personal Data Protection Regulations 2021 ("**PDP Regulations**")[36] • Advisory Guidelines on Key Concepts in the Personal Data Protection Act ("**PDPA Key Concepts Guidelines**")[37]
South Korea	**KR**	• Personal Information Protection Act ("**PIPA**")[38] • Enforcement Decree of the Personal Information Protection Act ("**Enforcement Decree**")[39] • Guidelines and Commentary on the Personal Information Protection Act ("**PIPA Guidelines**")[40]
Thailand	**TH**	• Personal Data Protection Act ("**PDPA**")[41] • PDPA Guidelines for Citizens[42] • Guidelines for obtaining consent for the personal data subject according to the PDPA ("**PDPA Consent Guidelines**")[43]
Vietnam	**VN**	• Draft Personal Data Protection Decree ("**Draft PDP Decree**") released for public consultation in 2020[44]

LEGAL BASES FOR PROCESSING PERSONAL DATA

Consent

All 14 of the jurisdictions studied recognize consent as a legal basis for processing personal data. Consent is not only a common denominator *across* these jurisdictions but also *within* their respective legal frameworks as in most cases, consent is the only legal basis that can be used to legitimize all activities involving personal data. By contrast, alternative legal bases to consent may only be available for certain activities involving personal data (see below).

In 6 of these jurisdictions (**Indonesia**, **Macau SAR**, **Malaysia**, the **Philippines**, **Singapore**, and **Vietnam**), consent is one of several equal legal bases for collection, use, and disclosure of personal data or depending on the terminology used in the relevant jurisdiction, "processing" of personal data.

In a further 4 jurisdictions (**China**, **India**, **South Korea**, and **Thailand**), consent is a legal basis for collection, use, and disclosure of personal data. In these jurisdictions, there may be several equal legal bases for certain activities involving personal data, but only a single legal basis for other such activities.

- In **China** and **South Korea**, consent is one of several legal bases for *collection* and *use* of personal data but is the sole legal basis for *disclosure* of personal data.
- Under **India**'s IT Rules, consent is the sole legal basis for processing "sensitive personal data or information" ("**SPDI**") but is one of several legal bases for disclosure of SPDI.
- In **South Korea** and **Thailand**, consent is one of several legal bases for collection of personal data *from the data subject* but is the sole legal basis for collection of personal data *from a third party*.
- In **Thailand**, consent is one of several legal bases for using personal data for a *primary purpose* but is the sole legal basis for using personal data for a *secondary purpose*.

In the remaining 4 jurisdictions (**Australia**, **Hong Kong SAR**, **Japan**, and **New Zealand**), consent is not a legal basis for collection, and use (and in some cases, disclosure) of personal data for a primary purpose. However, in these jurisdictions, consent may be a legal basis for certain specific activities involving personal data, such as:

- collection of personal data from a source other than the data subject (**Australia** and **New Zealand**);
- use or disclosure of personal data for a secondary purpose (**Australia**, **Hong Kong SAR**, **Japan**, and **New Zealand**);
- use of personal data for direct marketing purposes (**Australia** and **Hong Kong SAR**);
- in one case, disclosure of personal data to a third party for any purpose (**Japan**).

RELEVANT PROVISIONS

AUSTRALIA

Collection of personal information generally

Privacy Act, APP 3.2
An APP entity must not collect personal information (other than sensitive personal information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Privacy Act, APP 3.5
An APP entity must collect personal information only by lawful and fair means.

Collection of personal information from a source other than the data subject

Privacy Act, APPs 3.5
An APP entity must collect personal information about an individual only from the individual unless it is unreasonable or impracticable to do so.

Use or disclosure of personal information for a secondary purpose

Privacy Act, APP 6.1
If an APP entity holds personal information about an individual that was collected for a particular purpose (the ***primary purpose***), the entity must not use or disclose the information for another purpose (the ***secondary purpose***) unless:

- the individual has consented to the use or disclosure of the information; or
- an exception under APP 6.2 applies in relation to the use or disclosure of the personal information about the individual.

Use or disclosure of personal information for direct marketing

Privacy Act, APP 7
If an organization holds personal information about an individual, the organization must not use or disclose the information for the purpose of direct marketing.

Notwithstanding the above, an organization may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if either of the following exceptions applies.

Exception 1 — All of the following conditions must apply:

- the organization collected the information from the individual;
- the individual would reasonably expect the organization to use or disclose the information for the purpose of direct marketing;
- the organization provides a simple means by which the individual may easily request not to receive direct marketing communications from the organization; and
- the individual has not made such a request to the organization.

Exception 2 — All of the following conditions must apply:

- the organization collected the information from:
  - » the individual and the individual would not reasonably expect the organization to use or disclose the information for that purpose; or
  - » someone other than the individual;
- either:
  - » the individual has consented to the use or disclosure of the information for that purpose; or
  - » it is impracticable to obtain that consent;
- the organization provides a simple means by which the individual may easily request not to receive direct marketing communications from the organization;
- in each direct marketing communication with the individual:
  - » the organization includes a prominent statement that the individual may make such a request; or
  - » the organization otherwise draws the individual's attention to the fact that the individual may make such a request; and
- the individual has not made such a request to the organization.

RELEVANT PROVISIONS

CHINA

PIPL, Article 13(1)

Personal information handlers may handle an individual's personal information if they obtain the individual's consent.

PIPL, Article 25

Personal information handlers may not disclose the personal information that they handle except where they obtain separate consent.

HONG KONG SAR

Collection of personal data

PDPO, DPP 1(1)

Personal data may not be collected unless:

- the data is collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
- the collection of the data is necessary for or directly related to that purpose; and
- the data is adequate but not excessive in relation to that purpose.

PDPO, DPP 1(2)

Personal data must be collected by means that are lawful and fair in the circumstances of the case.

Use or disclosure of personal information for a secondary purpose

PDPO, DPP 3

Personal data may not, without the prescribed consent of the data subject, be used for any purpose other than the purpose for which the data was to be used at the time of the collection of the data or a purpose directly related thereto.

Note: The term "use," in relation to personal data, includes disclosure or transfer of the data (PDPO, Section 2(1)).

Use of personal data for direct marketing purposes

PDPO, Sections 35C(1)-(2), 35E, 35J, and 35K

A data user who intends to use a data subject's personal data in direct marketing, or provide a data subject's personal data to another person for use by that other person in direct marketing, must:

- inform the data subject that the data user:
  - » intends to so use or provide the personal data; and
  - » may not so use or provide the data unless the data user has received the data subject's consent to the intended use (which must be in writing if the data is to be provided to a third party);
- provide the data subject with the following information in relation to the intended use:
  - » the kinds of personal data to be used/provided;
  - » the classes of marketing subjects in relation to which the data is to be used; and
  - » if the data is to be provided to a third party,
    - twhether the data is provided for gain; and
    - the classes of persons to which the data is to be provided; and
- provide the data subject with a channel through which the data subject may, without charge by the data user, communicate the data subject's consent to the intended use or provision.

A data user who has complied with the above must not use the data subject's personal data in direct marketing or provide the data subject's personal data to another person for use by that other person in direct marketing unless:

- the data user has received the data subject's consent to the intended use or provision of personal data, as described in the information provided by the data user pursuant to the above, either generally or selectively; and
- the use is consistent with the data subject's consent.

If the consent for use of personal data for direct marketing is given orally, the data user must, within 14 days from receiving the consent, send a written confirmation to the data subject, confirming:

- the date of receipt of the consent;
- the permitted kind of personal data; and
- the permitted class of marketing subjects.

INDIA

Collection of sensitive personal data or information ("SPDI")

IT Rules, Rule 5
A body corporate or any person acting on its behalf must obtain consent in writing through letter, fax, or email from the provider of the SPDI regarding the body corporate's purpose for using that SPDI before collection of such SPDI.

When collecting SPDI directly from the person concerned, the body corporate or person on its behalf must take such steps as are, in the circumstances, reasonable to ensure that the person concerned has knowledge of:

- the fact that the SPDI is being collected;
- the purpose for which the SPDI is being collected;
- the intended recipients of the SPDI; and
- the name and address of the agency that:
  - is collecting the SPDI; and
  - will retain the SPDI.

Disclosure of SPDI

IT Rules, Rule 6(1)
Disclosure of SPDI by a body corporate to any third party requires prior permission from the provider of such information, subject to exceptions.

Draft DPDPB

Draft DPDPB, Section 5
A person may process the personal data of a data subject only for a lawful purpose for which the data subject has given, or is deemed to have given, consent according to the provisions of the Draft DPDPB.

INDONESIA

PDPL (2022), Article 20(a)
A personal data controller may process personal data where the data subject has given explicit consent for one or more specific purposes that the personal data controller has notified to the personal data subject.

JAPAN

APPI, Article 17
When handling personal information, a business operator handling personal information must specify the purpose of use as clearly as possible.

APPI, Article 18(1)
A business operator handling personal information must not, without the prior consent of the individual concerned, handle the individual's personal information beyond the scope necessary to achieve the purpose of use.

APPI, Article 19
Personal information providers must not use personal information in any way that may contribute to or induce illegal or unjust conduct.

APPI, Article 20

A business operator handling personal information must not acquire personal information through deception or other wrongful means.

Use of personal information for a secondary purpose

APPI, Article 17
A business operator handling personal information may not change the purpose of use beyond the scope that is reasonably considered to be relevant to the purpose of use before the change.

APPI, Article 18
A business operator handling personal information may not handle personal information beyond the scope necessary to achieve the purpose of use specified according to Article 17 of the APPI unless the business operator handling personal information obtains the prior consent of the individual, or an exception applies.

Disclosure of personal information to third party

APPI, Article 27
A business operator handling personal information may not provide personal data to a third party unless the business operator handling personal information obtains the prior consent of the individual, or an exception applies.

RELEVANT PROVISIONS

MACAU SAR

PDPA, Article 6

Personal data may be processed if the data subject has unambiguously given their consent.

MALAYSIA

PDPA, Section 6(1)(a)

A data user may process personal data about a data subject where the data subject has given consent to the processing of their personal data.

NEW ZEALAND

Collection of personal information

Privacy Act, IPP 1(1)

An agency must not collect personal information unless:

- the information is collected for a lawful purpose connected with a function or an activity of the agency; and
- the collection of the information is necessary for that purpose.

Privacy Act, IPP 4

An agency may collect personal information only by a means that:

- is lawful; and
- in the circumstances of the case:
  - » is fair; and
  - » does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Collection of personal information from a source other than the data subject

Privacy Act, IPP 2(1)

If an agency collects personal information, the information must be collected from the individual concerned.

IPP 2(2)(c)

An agency may collect personal information from a source other than the individual concerned if the agency believes, on reasonable grounds, that the individual concerned authorizes collection of the information from someone else.

Use of personal information for a secondary purpose

Privacy Act, IPP 10(1)(c)

An agency that holds personal information that was obtained in connection with one purpose may use the information for another purpose if thewe agency believes, on reasonable grounds, that the use of the information for that other purpose is authorized by the individual concerned.

Disclosure of personal information to a third party

Privacy Act, IPP 11(1)(c)

An agency that holds personal information may disclose the information to another agency or person where the agency believes, on reasonable grounds, that the disclosure is authorized by the individual concerned.

PHILIPPINES

DPA, Section 12(a)

The processing of personal information is permitted where the data subject has given their consent and where the processing is not otherwise prohibited by law.

IRRs, Section 21

For processing to be lawful, the data subject must have given their consent prior to the collection, or as soon as practicable and reasonable, or another legal basis must be available.

SINGAPORE

PDPA, Section 13(a)

An organization may collect, use, or disclose personal data about an individual where the individual gives, or is deemed to have given, consent to the collection, use, or disclosure.

SOUTH KOREA

Collection and use of personal information

PIPA, Article 15(1)(1)
A personal information controller may collect personal information and use it with the scope of the purpose of collection where consent is obtained from a data subject.

PIPA, Article 39-3(1)
An information and communications service provider who intends to collect and use personal information of users must notify users of certain prescribed matters and obtain consent therefor.

Collection of personal information from a third party

PIPA, Article 19(1)
A person who receives personal information from a personal information controller may not use the personal information or provide it to a third party for any purpose other than the original purpose unless additional consent is obtained from the data subject.

Disclosure of personal information

PIPA, Article 17(1)(1)
A personal information controller may provide the personal information of a data subject to a third party where consent is obtained from the data subject.

THAILAND

Collection, use, or disclosure of personal data generally

PDPA, Section 19
A data controller may collect, use, or disclose personal data where the data subject has given consent prior to or at the time of such collection, use, or disclosure.

Collection, use, or disclosure for a secondary purpose

PDPA, Section 21
A data controller must collect, use, or disclose personal data according to the purpose notified to the data subject prior to or at the time of such collection.

The collection, use, or disclosure of personal data may be conducted in a manner that is different from the purpose previously notified to the data subject, where the data subject has been informed of such new purpose, and consent is obtained prior to the time of collection, use, or disclosure.

Collection of personal data from a third party

PDPA, Section 25
A data controller may collect personal data from a source other than from the data subject directly where the data controller has informed the data subject of the collection of personal data from the other source without delay, and in any case, within 30 days of the date of such collection, and has obtained consent from the data subject.

Use or disclosure of personal data

PDPA, Section 27
A data controller may not use or disclose personal data without the consent of the data subject, unless the personal data was collected pursuant to an alternative legal basis to consent under Section 24 (in which case, the data controller must maintain a record of such use or disclosure pursuant to Section 39 of the PDPA).

VIETNAM

Draft PDP Decree, Article 3(4)

Personal data may be used with the consent of the data subject.

Conditions for consent

The data protection laws in 8 of the 14 jurisdictions studied (**China**, **India**, **Indonesia**, **Macau SAR**, the **Philippines**, **South Korea**, **Thailand**, and **Vietnam**) provide a detailed definition of consent or specify detailed requirements for valid consent. In 3 of these jurisdictions (**China**, the **Philippines**, and **South Korea**), guidelines and other guidance issued by relevant authorities offer more specific details on the conditions for consent.

By contrast, laws in the remaining 6 jurisdictions (**Australia**, **Hong Kong SAR**, **Japan**, **Malaysia**, **New Zealand**, and **Singapore**) either do not provide a definition or requirements for consent or provide only a limited definition or requirements. Guidelines issued by the relevant data protection authority in only 3 of these 6 jurisdictions (**Australia**, **Japan**, and **Singapore**) offer more specific conditions for consent.

Express Conditions for Consent in Laws, Regulations, and Guidelines

Across the 14 jurisdictions studied, there are 7 conditions for consent that are expressly stated in relevant laws, regulations, and guidelines. These requirements are outlined in Table 1 below.

There is significant divergence among the number of requirements recognized in each jurisdiction.

- **China** has the most conditions, followed by **Australia**, **Indonesia**, and **Thailand**, and then **South Korea** and **Macau SAR**.
- **New Zealand** has no express conditions for consent in its data protection laws and guidelines, and **Hong Kong SAR** has only a single condition.

Additionally, no single condition for consent is shared by all jurisdictions.

A majority of the jurisdictions in this category expressly require that consent must be voluntary in the sense that the consent is free from vitiating factors like mistake, misrepresentation, fraud, or duress.

Further, 10 of the 14 jurisdictions expressly require that consent must be informed (in at least certain circumstances).

- Six of these jurisdictions (**India**, **Indonesia**, **Singapore**, **South Korea**, **Thailand**, and **Vietnam**) specify the information that must be provided when seeking consent, whether through laws or guidelines.
- In the remaining jurisdictions (**Australia**, **China**, **Macau SAR**, and the **Philippines**), it is unclear how the requirement for informed consent interacts with broader notification requirements. For example, it is unclear whether failure to provide all items of information required by notification provisions would simply qualify as a breach of notification requirements or whether such failure would also render consent invalid (because the consent would not be "informed"). Assuming that consent is only informed when notification requirements have been complied with, it is also unclear whether it would still be necessary to obtain informed consent if an exception to notification requirements applies.

India, Indonesia, **Malaysia**, and **Vietnam** require that consent must be written or otherwise recorded. However, in **India** (IT Rules), this requirement extends only to consent for the collection of SPDI; there is no express requirement that consent for disclosure of SPDI must be recorded in writing.

Table 1: An overview of conditions for consent in the data protection laws, regulations and guidelines of 14 jurisdictions in Asia-Pacific

CONDITION FOR CONSENT	AU	CN	HK	IN	ID	JP	KR	MO	MY	NZ	PH	SG	TH	VN
Consent must be voluntary	✔	✔	✔	*	✘	✔	✔	✔	✘	✘	✘	✔	✔	✔
Consent must be informed	✔	✔	✔	*	✔	✘	✔	✔	✘	✘	✔	*	✔	✔
Consent must be specific	✔	*	✘	*	✔	✘	✔	✔	✘	✘	✔	✔	✔	✘
Consent must be written/recorded	✘	*	✘	*	✔	✔	✔	✘	✘	✘	✘	✘	✔	✔
Consent for processing of personal data must be separate from other matters	✘	*	✘	*	✔	✘	✔	✘	✘	✘	✘	✘	✔	✘
Consent must be explicit	✘	✔	✘	*	✔	✘	✘	✔	✘	✘	✘	✘	✔	✘
Consent must be current	✘	✘	✘	*	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘

**In certain circumstances.*

RELEVANT PROVISIONS

AUSTRALIA

Privacy Act, Section 6
Consent means either express or implied consent.

APP Guidelines, B.35
There are four necessary elements for consent under the APPs:

- the individual must be adequately informed before giving consent;
- the individual must give consent voluntarily;
- the consent given must be current and specific; and
- the individual must have the capacity to understand and communicate consent.

Informed consent

APP Guidelines, B.47
An individual must be aware of the implications of providing or withholding consent, such as whether access to a service will be denied if consent is not given for collection of a specific item of personal information. An APP entity should ensure that an individual is properly and clearly informed about how the individual's personal information will be handled, so the individual can decide whether to give consent. The information should be written in plain English, without legal or industry jargon.

Voluntary consent

APP Guidelines, B.43-44
Consent is given voluntarily if the consent is free from duress, coercion, or pressure that could overpower the individual's will. Relevant factors include:

- the alternatives available to the individual;
- the seriousness of any consequences; and
- any adverse consequences for family members or associates of the individual, if the individual does not give consent.

Current and specific consent

APP Guidelines, B.48-B.50
Consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely.

An APP entity should not seek a broader consent than is necessary for its purposes. When seeking consent, an entity should describe the purpose to which it relates. The level of specificity required will depend on the circumstances, including the sensitivity of the personal information.

CHINA

PIPL, Article 14

Where personal information is handled based on individual consent, the said consent must be given by individuals under the precondition of full knowledge, and in a voluntary and explicit statement. Where laws or administrative regulations provide that separate consent or written consent must be obtained to handle personal information, those provisions are to be followed.

HONG KONG SAR

Note: The PDPO recognizes different forms of consent ("prescribed consent" for use or disclosure of personal data for a secondary purpose under DPP 3) and consent for direct marketing under Part 6A of the PDPO.

PDPO, Section 2(3)

Where under the PDPO an act may be done with the prescribed consent of a person, such consent:

- means the express consent of the person given voluntarily; and
- does not include any consent that has been withdrawn by notice in writing served on the person to whom the consent has been given (but without prejudice to so much of that act that has been done pursuant to the consent at any time before the notice is so served).

PDPO, Section 35A(1)

Consent, in relation to use of personal data in direct marketing or a provision of personal data for use in direct marketing, includes an indication of no objection to the use or provision.

INDIA

Collection of SPDI

IT Rules, Rule 5

A body corporate or any person acting on its behalf must obtain consent in writing through letter, fax, or email from the provider of the SPDI regarding the body corporate's purpose for using that SPDI before collection of such SPDI.

When collecting SPDI directly from the person concerned, the body corporate or person on its behalf must take such steps as are, in the circumstances, reasonable to ensure that the person concerned has knowledge of:

- the fact that the SPDI is being collected;
- the purpose for which the SPDI is being collected;
- the intended recipients of the SPDI; and
- the name and address of the agency that:
  - » is collecting the SPDI; and
  - » will retain the SPDI.

Disclosure of SPDI

IT Rules, Rule 6(1)

Disclosure of SPDI by a body corporate to any third party requires prior permission from the provider of such information, subject to exceptions.

Draft DPDPB

Draft DPDPB, Section 7

Consent means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which the data subject, by a clear affirmative action, signifies agreement to the processing of the data subject's personal data for a specified purpose.

Every request for consent must be presented to the data subject in clear and plain language, together with the contact details of a data protection officer or other person authorized to respond to communication from the data subject for the purpose of exercising the data subject's rights under the Draft DPDPB. The data subject must be provided with the option to access such a request for consent in English or any language specified in the Eighth Schedule to the Constitution of India.

Draft DPDPB, Section 6

On or before requesting consent from a data subject, a "data fiduciary" must provide the data subject with an itemized notice in clear and plain language containing a description of the personal data sought to be collected and the purpose for processing such personal data.

INDONESIA

PDPL, Article 20(2)(a)

Processing of personal data is permitted where based on the explicit lawful consent of the personal data subject for one or more specific purposes communicated by the personal data controller to the personal data subject.

PDPL, Article 21
Where personal data is processed based on consent as pursuant to Article 20(2)(a) of the PDPL, the personal data controller must submit information regarding:

- the legality of the processing of personal data;
- the purposes of processing personal data;
- the type and relevance of personal data that will be processed;
- the retention period for documents containing personal data;
- details regarding the personal data collected;
- the period during which the personal data will be processed; and
- personal data subject's rights.

If there is a change to any of the above information, the personal data controller must notify the personal data subject prior to the change in the information.

PDPL, Article 22
Consent to the processing of personal data must be made in written or recorded form. Such consent has the same legal force whether it is submitted electronically or non-electronically.

If the consent contains other purposes, the request for consent must be:

- clearly distinguishable from other matter; and
- made in a format that is understandable and easily accessible, using simple and clear language.

Consent that does not satisfy the above requirements is declared null and void.

JAPAN

APPI Guidelines, section 2-16
Consent is defined as the individual's consent to the handling of personal information in the manner indicated by the business operator handling personal information. When obtaining consent, a business operator handling personal information must provide the individual with a reasonable and appropriate method to make a decision.

MACAU SAR

PDPA, Article 4(1)(9)
Consent of the data subject is any freely given, specific, and informed indication of the data subject's wishes by which the data subject signifies agreement to processing of personal data relating to the data subject.

PDPA, Article 6
Consent must be unambiguous.

MALAYSIA

Personal Data Protection Regulations 2013, Regulation 3
Consent can take any form that can be recorded and that the data user can properly maintain.

Consent for a specific form of processing of personal data must be distinguishable from other matters in the consent form.

NEW ZEALAND

The Privacy Act uses the term "authorization" rather than "consent" but does not define this term.

PHILIPPINS

DPA, Section 3(b)
The DPA defines the "consent of the data subject" as any freely given, specific, and informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to them.

SINGAPORE

PDPA, Section 13
An organization must not collect, use, or disclose personal data about an individual unless:

- the individual gives, or is deemed to have given, their consent under the PDPA to the collection, use, or disclosure; or
- the collection, use, or disclosure without the individual's consent is required or authorized under the PDPA or any other written law.

PDPA, Section 14 (actual consent)
An individual has not given consent under the PDPA for the collection, use, or disclosure of personal data about the individual by an organization for a purpose unless the individual:

- has been provided with the information required under Section 20 of the PDPA; and
- provided their consent for that purpose in accordance with the PDPA.
- An organization must not obtain or attempt to obtain consent for collecting, using, or disclosing personal data by providing false or misleading information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices.

PDPA, Section 15 (deemed consent)
An individual is deemed to consent to the collection, use, or disclosure of personal data about the individual by an organization for a purpose if:

- the individual, without actually giving consent mentioned in Section 14 of the PDPA, voluntarily provides the personal data to the organization for that purpose; and
- it is reasonable that the individual would voluntarily provide the data.

If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organization to another organization for a particular purpose, the individual is deemed to have consented to the collection, use, or disclosure of their personal data for that particular purpose by that other organization.

SOUTH KOREA

PIPA, Articles 15(2), 17(2), 18(3) (informed consent)
A personal information controller must inform a data subject of the following matters when it obtains consent pursuant to Article 15(1) (collection and use for primary purpose); Article 17(2) (disclosure); and Article 18(3) (use or disclosure for a secondary purpose) of the PIPA:

- the purpose of the collection and use of personal information;
- particulars of personal information to be collected, used, or disclosed;
- the recipient of personal information, if personal information is disclosed to a third party;
- the period for retaining and using personal information and, where personal information is disclosed to a third party, the period for retention and use by the recipient; and
- the fact that the data subject is entitled to deny consent and the disadvantages, if any, resulting from the denial of consent.

The personal information controller must also inform the data subject when any of the above information is modified.

PIPA, Article 16(2)
When collecting personal information on the basis of the data subject's consent, a personal information controller must specifically inform the data subject that the data subject may refuse to consent to the collection of any personal information that exceeds the minimum information necessary.

PIPA, Article 22(1)
For each matter requiring consent, a personal information controller must make a distinct request and obtain specific consent.

PIPA, Article 39-3(1)
Notwithstanding Article 15(1) of the PIPA, an information and communications service provider who intends to collect and use personal information of users must notify users of the following matters and obtain consent therefor:

- the purpose of the collection and use of personal information;
- particulars of personal information to be collected; and
- the period for retaining and using personal information.

The information and communications service provider must also inform the data subject when any of the above information changes.

PIPA Guidelines, page 82
Consent is the manifestation (e.g., written signature, oral confirmation, consent via an internet homepage) of a data subject's intent to voluntarily accept the collection or use of their personal information by the personal information controller. Such intent should be clearly ascertainable.

THAILAND

PDPA, Section 19

A request for consent must be explicitly made in a written statement, or via electronic means, unless this cannot be done by the nature of the request.

In requesting consent from the data subject, a personal data controller must inform the data subject of the purpose of the collection, use, or disclosure of the personal data.

A request for consent must be presented in a manner that is clearly distinguishable from other matters, in easily accessible and intelligible form and statements, using clear and plain language, and must not be deceptive or misleading to the data subject in respect to such a purpose.

In requesting consent from the data subject, the data controller must take the utmost care to ensure that the data subject's consent is freely given.

A request for the data subject's consent that is not in accordance with these provisions has no binding effect on the data subject and will not enable the data controller to collect, use, or disclose the personal data.

PDPA Guidelines for Citizens, page 3

Consent given in response to a request under Section 19 of the PDPA must be clear, unambiguous, and free in the sense that the data subject had an opportunity to make a genuine choice.

PDPC Consent Guidelines, Sections 3.1 and 3.4

A request for consent pursuant to Section 19 of the PDPA must be accompanied by the following information using language that is easy to understand:

- information about the personal data controller;
- the specific purpose for collecting, using, or disclosing the personal data;
- information about the type of personal data to be collected; and
- the existence of, and procedure for exercising, the data subject's right to withdraw consent.

Consent is not lawful if obtained through fraud, deception, intimidation, or misrepresentation.

VIETNAM

Draft PDP Decree, Article 8

Consent must also be given in a format that can be printed and reproduced in writing.

Draft PDP Decree, Article 13

Consent is only valid if given voluntarily and with knowledge of:

- the type of data to be processed;
- the purpose for processing;
- the parties permitted to process and share the data;
- the conditions for transferring and sharing the data to third parties; and
- the rights of data subjects in relation to the processing of their personal data according to law.

Express and implied consent

All 14 jurisdictions studied recognize express consent.

Recognition of Implied Consent

Three of the jurisdictions studied (**Australia, Japan**, and **Singapore**) recognize and provide for implied forms of consent.

In **Japan**, the APPI Q&A suggests that implied consent may be recognized in appropriate situations, where such consent is obtained using a reasonable and appropriate method that enables the data subject to make a decision regarding whether to give consent.[45] While the Q&A does not provide any specific examples of these situations, sectoral guidelines provide a number of examples of situations in which implied consent would be recognized.[46]

While **India**'s IT Rules do not appear to permit implied consent, the Draft DPDPB, if enacted in its current form, would recognize a form of implied consent where data subjects voluntarily provide their personal data to an organization, in circumstances where it is reasonable to expect that the data subject would do so.

The Draft DPDP Bill provides an illustration of how this provision would apply in practice: an individual who provides her name and mobile telephone number to an organization for the purpose of reserving a table at a restaurant would be deemed to have given her consent to the organization's collection of the name and number for the purpose of confirming the reservation.

RELEVANT PROVISIONS

AUSTRALIA

Privacy Act, Section 6
Consent is defined as either express or implied consent.

APP Guidelines, B.37-B.41
Express consent must be given explicitly, either verbally or in writing.

An individual's consent may be implied when it is reasonable to infer the individual's consent from the conduct of the individual and the APP entity in the circumstances. However, an APP entity should not assume that an individual has consented to collection, use, or disclosure of personal information simply on the basis that the collection, use, or disclosure appears to be advantageous to the individual or that the individual did not object to a proposal to handle personal information in a particular way.

In some circumstances, an opt-out option may be sufficient to show implied consent.

INDIA

Draft DPDPB, Section 8(1)
If enacted in its current form, the Draft DPDPB would deem consent to have been given for processing of the data subject's personal data, where such processing is necessary in a situation where the data subject voluntarily provides personal data to the data fiduciary, and it is reasonable to expect that the data subject would provide such personal data.

SINGAPORE

PDPA Key Concepts Guidelines, paragraphs 12.4 to 12.6
Consent may take different forms, including express consent as well consent that is implied or inferred from the circumstances.

Rejection of Implied Consent

A further 5 jurisdictions have rejected implied consent either expressly in their data protection laws (**Hong Kong SAR, India** (IT Rules), and **Vietnam**) or through guidance issued by data protection authorities (the **Philippines** and **Thailand**).

However, for **Hong Kong SAR**, this observation only applies to consent requirements for use or disclosure of personal data for a secondary purpose under DPP 3. A narrower definition of consent in Section s 35A(1) of the PDPO, which applies only in the context of direct marketing, permits opt-out consent.

HONG KONG SAR

PDPO, Section 2(3)

Where under the PDPO an act may be done with the prescribed consent of a person, such consent means the express consent of the person given voluntarily.

INDIA

Collection of SPDI

IT Rules, Rule 5

A body corporate or any person acting on its behalf must obtain consent in writing through letter, fax, or email from the provider of the SPDI regarding the body corporate's purpose for using that SPDI before collection of such SPDI.

When collecting SPDI directly from the person concerned, the body corporate or person on its behalf must take such steps as are, in the circumstances, reasonable to ensure that the person concerned has knowledge of:

- the fact that the SPDI is being collected;
- the purpose for which the SPDI is being collected;
- the intended recipients of the SPDI; and
- the name and address of the agency that:
  - is collecting the SPDI; and
  - will retain the SPDI.

THE PHILIPPINES

NPC Advisory Opinion No. 2017-007[47]

Implied, implicit, or negative forms of consent are not recognized under the DPA.

THAILAND

PDPA Consent Guidelines, Sections 3.6 and 4

A request for consent must be made expressly. Consent must take the form of an affirmative act involving an express statement of agreement to the collection, use, or disclosure of personal data.

VIETNAM

Draft PDP Decree, Article 8

Consent must also be given in a format that can be printed and reproduced in writing and cannot be inferred from silence or non-response of data subjects.

Status of Implied Consent Unclear

In the remaining jurisdictions, the status of implied consent is unclear, creating legal uncertainty.

China, **Indonesia**, **Macau SAR**, and **South Korea** do not expressly exclude implied consent, but it is unlikely that implied consent would satisfy their respective legislative conditions for consent, especially requirements that consent must be informed and explicit or specific (see above). However, note that **China**'s Security Specification notably recognizes consent given through a passive act — for example, where a person sees that a CCTV camera is recording but chooses to remain in view of the camera.[48]

In **Malaysia**, certain sectoral codes suggest that implied consent would be recognized in at least certain circumstances.[49] However, it is unclear if implied consent would be recognized more generally under the PDPA, especially as the Personal Data Protection Regulations 2013 require that consent must be capable of being recorded.

In **New Zealand**, several cases before the Privacy Commissioner and various Tribunals have rejected arguments relying on implied authorization. However, at least one case (*L v L* [2001] NZCRT 15) appeared to recognize implied authorization.[50]

Withdrawal of consent

Laws, regulations, and guidelines in 11 of the 14 jurisdictions in this category expressly provide for withdrawal of consent.

- **Australia, China**, and **Thailand** require entities to provide an easy and accessible method for withdrawing consent. By contrast, **Hong Kong SAR**, **India** (IT Rules), **Malaysia**, and **Singapore** require that consent be withdrawn by a written request.
- **Australia**, **Hong Kong SAR**, **Indonesia**, **Singapore**, **South Korea**, and **Thailand** expressly provide for the effect of withdrawal of consent.
  - » In **Hong Kong SAR**, **Malaysia**, and **South Korea**, an entity must cease processing personal data immediately on withdrawal of the consent. By contrast, **Indonesia** provides a window of 72 hours from this time, during which a personal data controller must cease processing.
  - » **Singapore** and **Thailand** require an organization to inform the data subject of the effect of withdrawing consent.

Three jurisdictions in this category (**Japan**, **Macau SAR**, and **New Zealand**) lack express provisions on withdrawal of consent. Though feedback from contributors indicates that it is generally understood in these jurisdictions that consent may be withdrawn,[51] there may be uncertainty as to an entity's responsibilities if consent is withdrawn.

RELEVANT PROVISIONS

AUSTRALIA

APP Guidelines, B.51

An individual may withdraw consent. APP entities must make withdrawal of consent an easy and accessible process and explain the potential implications of withdrawing consent.

Once an individual has withdrawn consent, an APP entity can no longer rely on past consent for any subsequent use or disclosure of the individual's personal information.

CHINA

PIPL, Article 15

Where personal information is handled based on individual consent, individuals have the right to rescind their consent. Personal information handlers must provide a convenient way to withdraw consent.

If an individual rescinds consent, it does not affect the effectiveness of personal information handling activities undertaken on the basis of individual consent before consent was rescinded.

HONG KONG SAR

PDPO, Section 2(3)

Consent may be withdrawn, in which case the data user should immediately terminate any processing activities that had been conducted on the basis of consent.

To withdraw "prescribed consent," the data subject must serve a notice in writing on the person to whom consent was given. Withdrawal of consent is without prejudice to acts done pursuant to consent before the notice of withdrawal is served.

INDIA

Collection of SPDI

IT Rules, Rule 5(7)

A provider of information has an option, at any time while using services or otherwise, to withdraw consent given earlier to a body corporate. Such withdrawal of consent must be sent in writing to the body corporate.

Draft DPDPB, Section 7
Where a data subject's personal data is processed on the basis of consent, the data subject has the right to withdraw consent at any time. The consequences of withdrawing consent shall be borne by the data subject. The withdrawal of consent does not affect the lawfulness of processing of the personal data based on consent before its withdrawal. The ease of such withdrawal must be comparable to the ease with which consent may be given.

If the data subject withdraws such consent, the data fiduciary must, within a reasonable time, cease, and cause its data processors to cease, processing of the personal data unless processing of the data without the data subject's consent is required or authorized by law.

INDONESIA

PDPL, Article 9
A personal data subject has the right to withdraw the consent to the processing of their personal data that has been given to a personal data controller.

PDPL, Article 40
If the personal data subject withdraws consent for the processing of personal data, the personal data controller must stop the processing of personal data no later than 72 hours from the time that the personal data controller receives the request to withdraw consent for the processing of personal data.

MALAYSIA

PDPA, Section 38
A data subject may withdraw their consent for the processing of their personal data by giving written notice to the data user. Upon receiving such a notice, the data user must cease processing the data subject's personal data.

PHILIPPINES

IRRs, Section 21
The data subject has a right to withdraw consent.

SINGAPORE

PDPA, Section 16
Organizations may not prohibit individuals from withdrawing consent.

Individuals may withdraw consent (including deemed consent) by giving reasonable notice to the organization.

On receiving such a notice, the organization must inform the individual of the likely consequences of withdrawing consent.

Once consent is withdrawn, the organization must cease (and cause its data intermediaries and agents to cease) collecting, using, or disclosing personal data, unless collection, use, or disclosure without the individual's consent is required or authorized under the PDPA or another written law.

SOUTH KOREA

PIPA, Article 37
A data subject has the right to request suspension of the processing of their personal information. Unless there are grounds for refusing such a request, the personal information controller must suspend the partial or entire processing of the data subject's personal information without delay.

PIPA Guidelines, page 381
The right in Article 37 of the PIPA is sufficiently broad to permit data subjects to withdraw consent for the processing of their personal information.

THAILAND

PDPA, Section 19
The data subject may withdraw their consent at any time. It must be as easy for the data subject to withdraw consent as to give consent unless there is a restriction on the withdrawal of consent by law or by a contract which gives benefits to the data subject.

Withdrawal of consent does not affect any collection, use, or disclosure of personal data for which the data subject has already legally given consent.

If the withdrawal of consent will affect the data subject in any manner, a data controller must inform the data subject of such consequences of withdrawing consent.

PDPA Guide for Citizens, page 7
Withdrawal of consent may take any form (e.g., electronic, written, etc.) provided that it is clear and easy to understand.

VIETNAM

Draft PDP Decree, Article 5(4)
Data subjects have a right to request that a personal data processor stop processing or disclosing personal data, except where processing or disclosure is required by law.

Draft PDP Decree, Article 8(7)
Consent can be withdrawn at any time.

Alternative legal basis to consent

All of the jurisdictions studied provide alternative legal bases to consent for processing personal data.

In **Australia**, **Hong Kong SAR**, **Japan**, and **New Zealand,** where consent plays a secondary role as a legal basis for certain activities involving personal data, alternative legal bases to consent exist in relation to processing personal data for those activities.

This Review has identified 26 unique legal bases for processing personal data without consent based on the express provisions of the data protection laws of the 14 jurisdictions studied. These legal bases are outlined in **Table 2** on the following page.

There is significant diversity as to the number of alternative legal bases to consent recognized by each jurisdiction:

- **Singapore** by far recognizes the most such bases, followed by **Hong Kong SAR**, then **Australia**, **China**, and **New Zealand**.
- **India** (IT Rules) recognizes the fewest such bases, followed by **Indonesia**, **Japan**, **Macau SAR**, and the **Philippines**.

Of the specific legal bases identified in this Review, all of the jurisdictions in this category permit processing of personal data without consent where necessary to protect the life or health of a person in at least certain circumstances.

All jurisdictions except **New Zealand** and **Singapore** recognize a general legal basis for processing personal data where necessary to comply with some form of legal obligation.

Approximately half of the jurisdictions studied provide legal bases for processing personal data without consent where necessary for entry into a contract or performance of obligations under a contract or for statistics and/or research.

Notably, a third of the legal bases identified in the cross-jurisdictional study are unique to a single jurisdiction and have no equivalents in other jurisdictions. In practice, many of these individual legal could be covered by broader legal bases in other jurisdictions (for example, jurisdictions which do not expressly recognize a legal basis for protecting public revenue may still permit processing of personal data without consent for this purpose under a broader legal basis, such as performing a task in the public interest) However, the lack of clarity increases the complexity, and likely cost, of cross-border compliance.

Table 2: An overview of alternative legal bases to consent for processing personal data in the data protection laws of 14 jurisdictions in Asia-Pacific

LEGAL BASIS	AU	CN	HK	IN*	ID	JP	KR	MO	MY	NZ	PH	SG	TH	VN
Necessity in an emergency or to protect the life or health of a person	✔	✔	✔	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Necessity to comply with legal obligations	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	✔	✘	✔	✔
Necessity to enter into, or perform an obligation under, a contract with the data subject	✘	✔	✘	✘	✔	✘	✔	✔	✔	✘	✔	✔	✔	✘
Statistics and/or research	✘	✘	✔	✘	✘	✘	✘	✘	✔	✔	✘	✔	✔	✔
Necessity for public health and/or safety	✔	✔	✘	✘	✘	✔	✘	✘	✘	✔	✔	✘	✘	✔
Processing authorized by law or regulation	✔	✔	✔	✘	✘	✔	✔	✘	✘	✘	✘	✔	✘	✔
Exercise of official or legal authority or performing a task in the public interest	✘	✘	✘	✘	✔	✘	✔	✔	✔	✘	✘	✘	✔	✘
Investigating and/or preventing crimes or misconduct	✔	✘	✔	✘	✘	✘	✘	✘	✘	✔	✘	✘	✔	✔
Necessity for legal proceedings and related purposes	✔	✘	✔	✘	✘	✘	✘	✘	✔	✔	✘	✔	✘	✘
News reporting in the public interest	✘	✔	✔	✘	✘	✘	✘	✘	✘	✘	✘	✔	✘	✔
Business transactions	✘	✘	✔	✘	✘	✘	✘	✘	✘	✔	✘	✔	✘	✘
Publicly available information	✘	✔	✘	✘	✘	✘	✘	✘	✘	✔	✘	✔	✘	✘
Establishing, exercising, or defending a legal claim or right	✔	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘	✔	✘	✘
Cooperating with government agencies	✘	✘	✘	✔	✘	✔	✘	✘	✘	✘	✘	✔	✘	✘
Necessity for human resources management	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘	✘	✔	✘	✘
Protecting national security	✘	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✔
Protecting public revenue	✔	✘	✘	✘	✘	✘	✘	✘	✘	✔	✘	✘	✘	✘
Locating missing persons	✔	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘
Calculating service fees	✘	✘	✘	✘	✘	✘	✔	✘	✘	✘	✘	✘	✘	✘
Business improvement purposes	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✔	✘	✘
Necessity for “evaluative purposes”	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✔	✘	✘
Necessity for recovery or payment of a debt	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✔	✘	✘
Credit reporting	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✔	✘	✘
Private trust or benefit plan	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✔	✘	✘
Providing a service for personal or domestic purposes	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✔	✘	✘

** IT Rules only. If enacted in its current form, the Draft DPDPB would introduce a number of new alternative legal bases to consent for processing personal data into India's personal data protection framework. However, note that the Draft DPDPB refers to these bases as forms of deemed consent.*

Necessity in an emergency or to protect the life or health of a person

Thirteen of the 14 jurisdictions studied currently permit processing of personal data without consent where necessary to protect the life or health of a person (this number will increase to 14 of 14 jurisdictions if **India** enacts the Draft DPDPB in its current form).

Prerequisites for Relying on the Legal Basis

Situations where consent would be inapplicable

Six of the 13 jurisdictions in this category (**Australia**, **Hong Kong SAR**, **Japan**, **Macau SAR**, **Singapore**, and **South Korea**) expressly state that the relevant legal basis may only be relied upon in situations where provisions for obtaining consent would be inapplicable because:

- consent cannot legally be obtained (for example, because the person lacks capacity to give consent or consent cannot be obtained from the person's legal representative);
- obtaining consent would cause harm to the person or a third party;
- the person would not be reasonably expected to withhold consent; or
- more broadly, other factors exist that would make it difficult, impractical, or unreasonable to obtain consent from the person.

Threshold for potential harm

There is divergence between jurisdictions as to:

- the risk of harm to protected interests that must exist as a threshold requirement for relying on this legal basis; and
- in some cases, the level of belief required on the part of the processing organization.

Five of the 13 jurisdictions in this category (**Indonesia**, **Japan**, **Macau SAR**, **Malaysia**, and the **Philippines**) simply permit the relevant legal basis to be relied on where necessary to protect the relevant interests without specifying a threshold for potential harm.

The remaining 7 jurisdictions in this category specify such a threshold but diverge based on the seriousness of potential harm.

- **Australia** and **New Zealand** require that an entity seeking to rely on the basis must have a reasonable belief that there is a "serious threat" to the protected interests. Similarly, **Singapore** permits such an entity to rely on the basis where minimally there are reasonable grounds to believe that the protected interests will be "seriously affected."
- **China** requires that there must be "emergency" conditions.
- **Hong Kong SAR** requires that there must be a likelihood of "serious harm."
- **South Korea** and **Thailand** both require that there must be a "danger" to the protected interests. **South Korea** additionally requires that the danger must be imminent.
- **Vietnam** requires that there must be a "urgency, threat to life, or a serious risk to the health of the data subject."

Range of Interests Protected

In four of the 13 jurisdictions in this category (**China**, **Japan**, **Malaysia**, and **South Korea**), the relevant legal basis expressly covers not only a person's bodily interests but also a person's security or property interests.

In a further 3 jurisdictions (**Indonesia**, **Macau SAR**, and the **Philippines**), the basis may also extend protection to these interests, depending on the interpretation of phrases like "vital interests" or "vitally important interests."

Parties Protected

Six of the 13 jurisdictions in this category (**Indonesia**, **Japan**, **Macau SAR**, **Malaysia**, the **Philippines**, and **Vietnam**) limit the scope of the basis to protection of the data subject's interests.

The remaining 7 jurisdictions (**Australia**, **China**, **Hong Kong SAR**, **New Zealand**, **Singapore**, **South Korea**, and **Thailand**) extend protection to any person. This means that in these jurisdictions, a data subject's personal data could be processed not only to protect the data subject himself/herself but also to protect third parties from the data subject where the data subject is potentially a danger to others, and seeking the data subject's consent could increase that risk or hinder efforts to apprehend the data subject.

Types of Personal Data Covered

In most jurisdictions in this category, the relevant legal basis applies to all types of personal data (other than sensitive personal data).

However, Section 59 of **Hong Kong SAR**'s PDPO is unique in that it applies only to personal data about the data subject's physical or mental health, identity, or location.

Informing Relevant Persons

Of the jurisdictions in this category, **Hong Kong SAR** and **Singapore** are unique in expressly providing legal bases for disclosure of the data subject's personal data to the data subject's family members or other relevant persons to inform such persons of the data subject's condition.

RELEVANT PROVISIONS

AUSTRALIA

Privacy Act, APP 6.2(c) read with Section 16A

Where an APP entity holds personal information about an individual that was collected for a primary purpose, and the individual has not consented to use or disclosure of that information for a secondary purpose, the APP entity may use or disclose the information for a secondary purpose if:

- it is unreasonable or impracticable to obtain the individual's consent to the use or disclosure; and
- the entity reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health, or safety of any individual.

CHINA

PIPL, Article 13(4)

Personal information handlers may handle personal information where necessary to protect natural persons' lives and health, or the security of their property, under emergency conditions.

HONG KONG SAR

PDPO, Section 59

Personal data relating to the physical or mental health or the identity or location of a data subject may be used or disclosed for a secondary purpose without the data subject's consent if seeking consent for such use or disclosure would be likely to cause serious harm to the physical or mental health of the data subject or any other individual.

PDPO, Section 63C

Personal data may be used or disclosed for a secondary purpose without the data subject's consent if seeking consent for such use or disclosure would be likely to prejudice any of the following matters:

- identifying an individual who is reasonably suspected to be, or is, involved in a life-threatening situation;
- informing the individual's family members or relevant persons of the individual's involvement in the life-threatening situation; or
- the carrying out of emergency rescue operations or provision of emergency relief services.

INDIA

Draft DPDPB, Section 8(4)

If enacted in its current form, the Draft DPDPB would deem consent to have been given for processing of the data subject's personal data, where such processing is necessary for responding to a medical emergency involving a threat to the life of, or immediate threat to the health of, the data subject or any other individual.

INDONESIA

PDPL, Article 20(2)(d)

A personal data controller may process personal data for fulfillment of the protection of the vital interests of the personal data subject.

JAPAN

APPI, Articles 18(2)(ii) (use for a secondary purpose) and 27(1)(ii) (disclosure)

A business operator handling personal information may handle an individual's personal information beyond the scope necessary to achieve the purpose of use or disclose an individual's personal information to a third party without obtaining the individual's prior consent, where such use or disclosure is necessary for the protection of the life, body, or property of an individual, and it is difficult to obtain the consent of the individual.

MACAU SAR

PDPA, Article 6(3)

Personal data may be processed where processing is necessary to protect the vital interests of the data subject, and the data subject is physically or legally incapable of giving consent.

MALAYSIA

PDPA, Section 6(2)(d)

A data user may process personal data about a data subject if the processing is necessary to protect the "***vital interests***" of the data subject.

Note: "***vital interests***" is defined as matters relating to life, death, or security of a data subject (PDPA, s 4).

NEW ZEALAND

Privacy Act, IPP 10(1)(f)(ii)

An agency that holds personal information that was obtained in connection with one purpose may use the information for any another purpose if the agency believes, on reasonable grounds, that the use of the information for that other purpose is necessary to prevent or lessen a serious threat to the life or health of the individual concerned or another individual.

PHILIPPINES

DPA, Section 12(d)

The processing of personal information is permitted where necessary to protect vitally important interests of the data subject, including life and health.

SINGAPORE

PDPA, First Schedule, Part 1

An organization may collect, use, or disclose personal data about an individual where:

- the collection, use, or disclosure is necessary:
  - for any purpose that is clearly in the individual's interests, and consent for the collection, use, or disclosure cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent; or
  - to respond to an emergency that threatens the life, health, or safety of the individual or another individual;
- consent for the collection, use, or disclosure cannot be obtained in a timely way, and there are reasonable grounds to believe that the health or safety of the individual or another individual will be seriously affected; or
- the collection, use, or disclosure of personal data is for the purpose of contacting the next-of-kin or a friend of any injured, ill, or deceased individual.

SOUTH KOREA

PIPA, Article 15(1)(5)

A personal information controller may collect personal information and use it within the

scope of the purpose of collection where such collection or use is deemed manifestly necessary for the protection of life or bodily or property interests of the data subject or a third party from imminent danger where the data subject or their legal representative is not in a position to express intention, or prior consent cannot be obtained.

PIPA, Article 17(1)(2)
A personal information controller may provide the personal information of a data subject to a third party where the personal information is provided within the scope of purposes for which it is collected pursuant to Article 15(1)(5) of the PIPA.

THAILAND

PDPA, Section 24(2)
A data controller may collect personal data without the consent of the data subject where the collection is for preventing or suppressing a danger to a person's life, body, or health.

VIETNAM

Draft PDP Decree, Articles 6(1)(đ)
Personal data processors and third parties may disclose personal data without the consent of the data subject where disclosure is required by law based on urgency, threat to life, or serious risk to the health of the data subject.

Draft PDP Decree, Article 10(1)(c)
Personal data may be processed without the consent of the data subject where processing is required by law based on urgency, threat to life, or serious risk to the health of the data subject.

Necessity to comply with a legal obligation

Twelve of the 14 jurisdictions studied permit processing of personal data without consent where required by law or where necessary to comply with legal obligations, including those in:

- legislative instruments, such as laws, regulations, and statutes;
- court orders; and
- international agreements or treaties (**Vietnam**).

Only **New Zealand** and **Singapore** lack a general legal basis for this purpose.

RELEVANT PROVISIONS

AUSTRALIA

Privacy Act, DPP 6.2(b)
An APP entity may use or disclose the information for a secondary purpose if such use or disclosure is required by or under an Australian law or a court/tribunal order.

CHINA

PIPL, Article 13(3)
Personal information handlers may handle personal information where necessary to fulfill statutory duties, responsibilities, or obligations.

HONG KONG SAR

PDPO, Section 60B(a)
Personal data is exempt from the provisions of DPP 3 if the use of the data is required by or under any enactment by any rule of law or by an order of a court in Hong Kong SAR.

INDIA

IT Rules, Rule 6 (disclosure)

A body corporate may disclose SPDI to any third party without prior permission from the provider of such information where the disclosure is necessary to comply with a legal obligation.

Draft DPDPB, Section 8(3)

If enacted in its current form, the Draft DPDPB would deem consent to have been given for processing of the data subject's personal data, where such processing is necessary for compliance with any judgment or order issued under any law.

INDONESIA

PDPL, Article 20(2)(c)

A personal data controller may process personal data to fulfill the personal data controller's legal obligations according to the provisions of laws and regulations.

JAPAN

APPI, Articles 18(2)(i) (use) and 27(1)(i) (disclosure)

A business operator handling personal information may handle an individual's personal information beyond the scope necessary to achieve the purpose of use or disclose an individual's personal information to a third party, without obtaining the individual's prior consent where such handling or disclosure is required by law.

MACAU SAR

PDPA, Article 6(2)

Personal data may be processed if processing is necessary to comply with a legal obligation to which the controller is subject.

MALAYSIA

PDPA, Section 6(2)(c)

A data user may process personal data about a data subject if such processing is necessary to comply with any legal obligation to which the data user is subject, other than an obligation imposed by a contract.

PHILIPPINES

DPA, Section 12(c)

The processing of personal information is permitted where necessary to comply with a legal obligation to which the personal information controller is subject.

SOUTH KOREA

PIPA, Article 15(1)(5)

A personal information controller may collect personal information and use it within the scope of the purpose of collection where such collection or use is unavoidable to observe legal obligations.

Article 17(1)(2)

A personal information controller may disclose the personal information of a data subject to a third party where the disclosure is within the scope of the purposes for which the personal data was collected pursuant to Article 15(1)(5) of the PIPA.

THAILAND

PDPA, Section 24(6)

A data controller may collect personal data without the consent of the data subject where such collection is necessary to comply with a law to which the data controller is subject.

VIETNAM

Draft PDP Decree, Article 10(1)(đ) (treaties)

Personal data may be processed without the consent of the data subject to implement specific regulations stating the permission to process personal data without the consent of the data subject in international agreements or treaties to which Vietnam is a signatory.

Necessity to enter into, or perform an obligation under, a contract with the data subject

Eight of the 14 jurisdictions studied permit processing of personal data where necessary to either:

- take steps to enter into a contract with the data subject; or
- perform an obligation under a contract with the data subject.

All jurisdictions in this category minimally permit processing of personal data where necessary to perform obligations under a contract to which the data subject is a party or is subject.

However, these jurisdictions differ slightly in terms of the precontractual activities for which personal data may be processed without consent.

Most jurisdictions in this category permit such processing where necessary to fulfill, or take steps to fulfill, a request from the data subject before entering into a contract with the data subject.

By contrast, **China** and **South Korea** do not refer to requests from the data subject and instead, permit processing of personal data where generally necessary to "conclude" or "execute" a contract with the data subject.

Additionally, **South Korea** only permits information and communications service providers to collect and use personal data without consent on this basis where it is clearly difficult to obtain ordinary consent for economic and technical reasons.

Singapore is unique in framing its legal basis as a form of deemed consent. However, the relevant provision functions similarly to the other legal bases in this category, albeit in a narrower scope.

RELEVANT PROVISIONS

CHINA

PIPL, Article 13(2)

Personal information handlers may handle personal information where necessary to conclude or fulfill a contract in which the individual is an interested party.

INDONESIA

PDPL, Article 20(2)(b)

A personal data controller may process personal data to fulfill obligations under an agreement to which the personal data subject is one of the parties or to fulfill the request of the personal data subject when entering into an agreement.

MACAU SAR

PDPA, Article 6(1)

Personal data may be processed if processing is necessary for the performance of a contract or contracts to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract or a declaration of their will to negotiate.

MALAYSIA

PDPA, Section 6(2)(a)-(b)

A data user may process personal data about a data subject if the processing is necessary for:

- the performance of a contract to which the data subject is a party; or
- the taking of steps at the request of the data subject with a view to entering into a contract.

PHILIPPINES

DPA, Section 12(b)

The processing of personal information is permitted where necessary for and related to the fulfillment of a contract with the data subject or to take steps at the request of the data subject prior to entering into a contract.

SINGAPORE

PDPA, Section 15

An individual (*P*) who provides personal data to an organization (*A*) with a view to *P* entering into a contract with *A* is deemed to consent to the following where reasonably necessary for the conclusion of the contract between *P* and *A*:

- the disclosure of that personal data by A to another organization (B);
- the collection and use of that personal data by *B*;
- the disclosure of that personal data by *B* to another organization (*C*).

Where *C* collects personal data disclosed to *C* by *B* pursuant to the above provision, *P* is deemed to consent to:

- the collection and use of that personal data by *C*;
- the disclosure of that personal data by *C* to yet another organization.

Without limiting the above provisions, an individual (*P*) who enters into a contract with an organization (*A*) and provides personal data to *A* pursuant or in relation to that contract is deemed to consent to the following:

- the disclosure of that personal data by *A* to another organization (*B*), where the disclosure is reasonably necessary for either of the following purposes ("**relevant purpose**"):
  - » the performance of the contract between *P* and *A*; or
  - » the conclusion or performance of a contract between *A* and *B* that is entered into at *P*'s request, or that a reasonable person would consider to be in *P*'s interest;
- the collection and use of that personal data by *B*, where the collection and use are reasonably necessary for a relevant purpose; and
- the disclosure of that personal data by *B* to another organization (*C*), where the disclosure is reasonably necessary for a relevant purpose.

Where *C* collects personal data disclosed to *C* by *B* pursuant to the above provision, *P* is deemed to consent to:

- the collection and use of that personal data by *C*, where the collection and use are reasonably necessary for a relevant purpose; and
- the disclosure of that personal data by *C* to yet another organization, where the disclosure is reasonably necessary for a relevant purpose.

These subsections do not affect any obligation under the contract between *P* and *A* that specifies or restricts:

- the personal data provided by *P* that *A* may disclose to another organization; or
- the purposes for which *A* may disclose the personal data provided by *P* to another organization.

SOUTH KOREA

PIPA, Article 15(1)(4)

A personal information controller may collect personal information and use it within the scope of the purpose of collection where such collection or use is unavoidably necessary to execute and perform a contract with a data subject.

PIPA, Article 39-3(2)(1)

An information and communications service provider may collect and use personal information of users without their consent where the information is necessary to implement a contract for provision of information and communications services, but it is clearly difficult to obtain ordinary consent for economic and technical reasons.

THAILAND

PDPA, Section 24(3)

A data controller may collect personal data without the consent of the data subject where such collection is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering into a contract.

Statistics and/or research

Six of the 14 jurisdictions studied permit processing of personal data without consent for statistical and/or research purposes, subject to implementation of prescribed safeguards.

Permitted Purposes

While all 6 jurisdictions in this category permit processing of personal data for statistical and/or research purposes, there are minor differences in terminology between jurisdictions.

- **Singapore** and **Thailand** expressly refer to research for archival or historical research purposes.
- **Vietnam** refers only to scientific research.

Research in the Public Interest

Of the 6 jurisdictions in this category, 2 jurisdictions (**Singapore** and **Thailand**) specifically require that research must be in the public interest or for public benefit. The remaining 4 jurisdictions lack such a requirement.

Required Safeguards

All jurisdictions in this category require entities seeking to rely on this legal basis to implement specific safeguards.

Unlike the data protection laws of other jurisdictions in this category, **Thailand**'s PDPA does not specify these safeguards in legislation. Rather, the relevant provision requires entities to comply with guidelines issued by Thailand's Personal Data Protection Commission. As of the date of this Review, the Commission has not issued guidelines as to processing of personal data for statistical or research purposes.

The 5 of the remaining jurisdictions in this category minimally require that the statistics and/or research must not identify any of the data subjects.

- The relevant provisions in **Hong Kong SAR**, **Malaysia**, **New Zealand**, and **Singapore** do not strictly prohibit processing of personally identifiable information but specify that the *resulting statistics or research* may not be released in any form that identifies, or may identify, any of the data subjects.
- By contrast, the relevant provisions in **Vietnam** are far more stringent, requiring that the personal data must be encrypted and pseudonymized before it is processed for statistical or research purposes and prohibiting any forms of processing that could identify data subjects through aggregation.

Hong Kong SAR, **Malaysia**, and **Singapore** also prohibit processing of personal data on this basis for any purpose other than statistics and/or research.

Lastly, **Singapore** and **Vietnam** each impose several additional safeguards that are not required by other jurisdictions in this category.

- **Singapore** specifies a standard of 'reasonable necessity' for processing personal data in an individually identifiable form, and prohibitions on:
  - using the results of research to make decisions about the individual; and
  - processing personal data for archival or historical purposes if a reasonable person would consider processing of the personal data to be too sensitive at the proposed time.
- **Vietnam** requires the implementation of several organizational measures to protect personal data processed for statistical or research purposes, and also written confirmation from the Personal Data Protection Commission that such measures have been implemented.

RELEVANT PROVISIONS

HONG KONG SAR

PDPO, Section 62

Personal data is exempt from the provisions of DPP 3 where:

- the data is to be used for preparing statistics or carrying out research;
- the data is not to be used for any other purpose; and
- the resulting statistics or results of the research are not made available in a form that identifies any data subject.

MALAYSIA

PDPA, Section 45(2)(c)

Personal data processed for preparing statistics or carrying out research is exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of the PDPA, provided that such personal data is not processed for any other purpose and that the resulting statistics or the results of the research are not made available in a form that identifies the data subject.

NEW ZEALAND

Privacy Act, IPP 10(1)(b)(ii) (use for a secondary purpose) and IPP 11(1)(h)(ii) (disclosure)

An agency may use personal information for a secondary purpose or disclose the information to a third party where the agency believes, on reasonable grounds, that the information is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

SINGAPORE

PDPA, First Schedule, Part 2, paragraph 4

An organization may collect, use, or disclose ersonal data about an individual if the collection, use, or disclosure is solely for archival or historical purposes, and a reasonable person would not consider the personal data to be too sensitive to be collected, used, or disclosed at the proposed time.

PDPA, Second Schedule, Part 2, Division 3

An organization may use personal data about an individual for a research purpose, including historical or statistical research, if:

- the research purpose cannot reasonably be accomplished unless the personal data is used in an individually identifiable form;
- there is a clear public benefit to using the personal data for the research purpose;
- the results of the research will not be used to make any decision that affects the individual; and
- if the results of the research are published, the organization publishes the results in a form that does not identify the individual.

THAILAND

PDPA, Section 24(1)

A data controller may collect personal data without the consent of the data subject if such collection is for the achievement of a purpose relating to the preparation of historical documents or archives in the public interest, or for a purpose relating to research or statistics, provided that appropriate measures to safeguard the data subject's rights and freedoms as prescribed by the Commission have been put in place.

VIETNAM

Draft PDP Decree, Articles 10(1) and 12

Personal data may be processed without the consent of the data subject where the processing is in service of scientific research or statistics according to the provisions of Article 12 of the Draft PDP Decree.

Draft PDP Decree, Article 12

- The personal data must be processed in encrypted form.
- Before handing over personal data for data processing for scientific research or statistics, data identifying a person must be de-identified and replaced with a code. Decoding and decoding capabilities are only permitted for scientific or statistical research. The personal data processor

must designate in writing a specific person who has access to the information allowing for decryption.

- The results of processing personal data for scientific research or statistics cannot be aggregated into information of a particular data subject.
- The processing should fully implement the following:
  - a commitment to protect personal data;
  - measures to secure personal data;
  - a physical device to protect personal data;
  - a specialized department assigned the task of protecting personal data; and
  - registration with the Personal Data Protection Commission to handle sensitive personal data.

There must be a written confirmation from the Personal Data Protection Commission that the above conditions have been fulfilled.

Necessity for public health and/or safety

In addition to the legal bases for protecting the life or health of a person shared by all jurisdictions (see above), data protection laws in 6 of the 14 jurisdictions studied also expressly provide legal bases for processing of personal data where necessary for public health and/or safety. This number will increase to 7 of 14 jurisdictions if India enacts the Draft DPDPB in its current form.

Prerequisites for Relying on the Legal Basis

Situations where consent would be inapplicable

Of the 6 jurisdictions in this category, 2 jurisdictions (**Australia** and **Japan**) limit the application of this legal basis to situations where consent is inapplicable. Specifically, **Japan** requires that it be difficult to obtain consent, while **Australia** requires that it must be unreasonable or impractical to obtain consent.

Threshold for potential harm

There is divergence between jurisdictions as to:

- the risk of harm to protected interests that must exist as a threshold requirement for relying on this legal basis; and
- in some cases, the level of belief required on the part of the entity.

Australia and **New Zealand** require that an entity seeking to rely on this legal basis must *reasonably believe* that there is a "serious threat" to public health or safety. By contrast, **Vietnam** requires that there must be a "serious risk" to public health while the Philippines requires that there must be an emergency.

Japan is unique in that the focus of its legal basis is inverted, concentrating on improving public health rather than avoiding harm to public health.

Protected Interests

The jurisdictions in this category also differ according to the interests that they protect.

The relevant legal bases in **Australia** and **New Zealand** protect both public health and public safety, while those in **China**, **Japan**, and **Vietnam** protect only public health.

By contrast, the relevant legal basis in the **Philippines** protects only public safety.

RELEVANT PROVISIONS

AUSTRALIA

Privacy Act, APP 6.2(c) read with Section 16A

An APP entity may use or disclose the information for a secondary purpose where:

- it is unreasonable or impracticable to obtain the individual's consent to the use or disclosure; and
- the entity reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to public health or public safety.

CHINA

PIPL, Article 13(4)

Personal information handlers may handle personal information where necessary to respond to sudden public health incidents.

INDIA

Draft DPDPB, Sections 8(5) and 8(6)

If enacted in its current form, the Draft DPDPB would deem consent to have been given for processing of the data subject's personal data, where such processing is necessary for taking measures to:

- provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health; or
- ensure the safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order.

JAPAN

APPI, Articles 18(2)(iii) (use) and 27(1)(iii) (disclosure)

A business operator handling personal information may handle an individual's personal information beyond the scope necessary to achieve the purpose of use, or disclose an individual's personal information to a third party, without obtaining the individual's prior consent where the disclosure is particularly necessary for improving public health or promoting the sound growth of children and where it is difficult to obtain the consent of the individual.

NEW ZEALAND

Privacy Act, IPP 10(1)(f)(i) (use for a secondary purpose) and **IPP 11(1)(f)(i) (disclosure)**

An agency may use personal information for a secondary purpose or disclose the information to a third party where the agency believes, on reasonable grounds, that such use or disclosure is necessary to prevent or lessen a serious threat to public health or public safety.

PHILIPPINES

DPA, Section 12(e)

The processing of personal information is permitted if necessary to respond to national emergencies or to comply with the requirements of public order and safety, provided that the processing is not otherwise prohibited by law.

VIETNAM

Draft PDP Decree, Articles 6(1)(đ)

Personal data processors and third parties may disclose personal data without the consent of the data subject where disclosure is required by law based on serious risk to public health.

Draft PDP Decree, Article 10(1)(c)

Personal data may be processed without the consent of the data subject where processing is required by law based on serious risk to public health.

Processing authorized by law or regulation

Six of the 14 jurisdictions studied permit processing of personal data without consent where such processing is *permitted* by laws, regulations, or in some cases, court orders.

This legal basis is distinct from the legal basis where processing is necessary to comply with legal obligations under (i.e., *required* by) such legal instruments.

RELEVANT PROVISIONS

AUSTRALIA

Privacy Act, DPP 6.2(b)

An APP entity may use or disclose the information for a secondary purpose if such use or disclosure is authorized by or under an Australian law or a court/tribunal order.

CHINA

PIPL, Article 13(7)

Personal information handlers may handle personal information where laws and administrative regulations provide for such processing.

HONG KONG SAR

PDPO, Section 60B(a)

Personal data is exempt from the provisions of DPP 3 if the use of the data is authorized by or under any enactment, by any rule of law or by an order of a court in Hong Kong SAR.

SINGAPORE

PDPA, Section 13

An organization may collect, use, or disclose personal data about an individual if the collection, use, or disclosure without the individual's consent is required or authorized under the PDPA or any other written law.

SOUTH KOREA

PIPA, Articles 15(1)(2) and 17(1)(2)

A personal information controller may collect personal information and use it within the scope of the purpose of collection, or may disclose personal information to a third party, where other laws specifically provide for such collection, use, or disclosure.

PIPA, Article 39-3(2)(3)

An information and communications service provider may collect and use personal information of users without users' consent where other laws specifically provide for such collection or use.

VIETNAM

Draft PDP Decree, Articles 6(1)(a)

Personal data processors and third parties may disclose personal data without the consent of the data subject where such disclosure is made according to the provisions of law.

Draft PDP Decree 10(1)(a)

Personal data may be processed without the consent of the data subject where such processing is according to the provisions of law.

Exercise of official or legal authority or performing a task in public interest

Six of the 14 jurisdictions studied permit processing of personal data where such processing is:

- in the exercise of official or legal authority; and/or
- necessary for performing a task in the public interest.

This number will increase to 6 of 14 jurisdictions if India enacts the Draft DPDPB in its current form.

Of the 5 jurisdictions in this category, 3 (**Indonesia**, **Macau SAR**, and **Thailand**) permit such processing in either of the above situations. By contrast, 2 jurisdictions (**Malaysia** and **South Korea**) only permit such processing in the exercise of official or legal authority. In the case of **South Korea**, the relevant legal basis applies only to public institutions acting within the scope of their statutory duties. Notably, the relevant legal basis in **Malaysia** is broader than its equivalents in other jurisdictions in this category as it permits processing where necessary for the exercise of any functions legally conferred "on any person."

All jurisdictions in this category except **Singapore** require that the processing must be necessary for either or both of these purposes.

RELEVANT PROVISIONS

INDIA

Draft DPDPB, Section 8(2)

If enacted in its current form, the Draft DPDPB would deem consent to have been given for processing of the data subject's personal data, where such processing is necessary for the performance of any function under any law, or the provision of any service or benefit to the data subject, or the issuance of any certificate, license, or permit for any action or activity of the data subject, by the State or any instrumentality of the State.

INDONESIA

PDPL, Article 20(2)(e)

A personal data controller may process personal data for the exercise of its authority or performance of its duties in the public interest based on laws and regulations.

MACAU SAR

PDPA, Article 6(4)

Personal data may be processed where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed.

MALAYSIA

PDPA, Section 6(2)(f)

A data user may process personal data about a data subject if the processing is necessary for the exercise of any functions conferred on any person by or under any law.

SOUTH KOREA

PIPA, Article 15(1)(3)

A personal information controller may collect personal information and use it with the scope of the purpose of collection where such collection or use is unavoidable for the performance by a public institution of its duties within its jurisdiction as prescribed by statutes.

Article 17(1)(2)

A personal information controller may provide the personal information of a data subject to a third party where the personal information is provided within the scope of purposes for which it is collected pursuant to Article 15(1)(3) of the PIPA.

THAILAND

PDPA, Section 24(4)

A data controller may collect personal data without the consent of the data subject where such collection is necessary for the performance of a task carried out in the public interest by the data controller or the exercise of official authority vested in the data controller.

Investigating and/or preventing crimes or misconduct

Six of the 14 jurisdictions studied permit processing of personal data without consent for various purposes relating to investigating, preventing, and taking action in relation to crimes or misconduct. This number will increase to 6 of 14 jurisdictions in **India** enacts the Draft DPDPB in its current form.

Across the jurisdictions in this category, all of the relevant legal bases appear to relate to law enforcement-related activities by relevant public or professional bodies, whether or not the relevant provisions expressly refer to such bodies. However, **Australia** notably also provides a legal basis for processing that would permit private entities to identify misconduct relating to the entities' functions or activities and take appropriate action, which may include pursuing a civil remedy.

All jurisdictions in this category except **Singapore** provide legal bases for both the investigation and broader prevention and remediation of crimes and/or misconduct. By contrast, **Singapore**'s provision applies only to investigation.

Further, the relevant legal bases of three jurisdictions in this category (**Australia**, **New Zealand**, and **Singapore**) include express necessity requirements. By contrast, the legal bases in **Hong Kong SAR** and **Vietnam** require that the processing of personal data without the data subject's consent must be for any of the prescribed purposes. However, as a safeguard, the provision in **Hong Kong SAR** only permits such processing where obtaining the data subject's consent would prejudice any of the prescribed, law-enforcement related purposes.

RELEVANT PROVISIONS

AUSTRALIA

Privacy Act, APP 6.2(c) read with Sections 6(1) and 16A

An APP entity may use or disclose personal information for a secondary purpose where:

- the entity has reason to suspect that unlawful activity, or "***misconduct***" of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in; and
- the entity reasonably believes that the use or disclosure is necessary for the entity to take appropriate action in relation to the matter.

Note: "***misconduct***" includes fraud, negligence, default, breach of trust, breach of duty, breach of discipline, or any other misconduct in the course of duty.

Privacy Act, APP 6.2(e) read with Section 6(1)

An APP entity may use or disclose personal information for a secondary purpose if the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more "***enforcement related activities***" conducted by, or on behalf of, an "***enforcement body***."

Note: "***enforcement body***" covers numerous public authorities tasked with investigating and enforcing crimes and regulatory offenses, including state, territory, and federal police.

An "***enforcement related activity***" means:

- the prevention, detection, investigation, prosecution, or punishment of:
  - » criminal offenses; or
  - » breaches of a law imposing a penalty or sanction;
- the conduct of surveillance activities, intelligence gathering activities, or monitoring activities;

- the conduct of protective or custodial activities;
- the enforcement of laws relating to the confiscation of the proceeds of crime;
- the protection of the public revenue;
- the prevention, detection, investigation, or remedying of misconduct of a serious nature, or other conduct prescribed by regulation;
- the preparation for, or conduct of, proceedings before any court or tribunal, or the implementation of court/tribunal orders.

HONG KONG SAR

PDPO, Section 58(2)

Personal data may be used or disclosed for a secondary purpose without the data subject's consent if:

- the use of the data is for any of the following purposes (whether or not the data is held for any of those purposes);
  - » the prevention or detection of crime;
  - » the apprehension, prosecution, or detention of offenders;
  - » the assessment or collection of any tax or duty;
  - » the prevention, preclusion, or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;
  - » the prevention or preclusion of significant financial loss arising from:
    - any imprudent business practices or activities of persons; or
    - unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;
  - » ascertaining whether the character or activities of the data subject are likely to have a significantly adverse impact on any thing:
    - to which the discharge of statutory functions by the data user relates; or
    - which relates to the discharge of functions to which this paragraph applies; or
  - » discharging functions to which this paragraph applies; and
- obtaining the data subject's consent in relation to such use would be likely to prejudice any of the above matters.

INDIA

Draft DPDPB, Section 8(8)(a)

If enacted in its current form, the Draft DPDPB would deem consent to have been given for processing of the data subject's personal data, where such processing is necessary in the public interest, including for prevention and detection of fraud.

NEW ZEALAND

Privacy Act, IPP 10(1)(e)(i)-(ii) (use for a secondary purpose) and IPP 11(1)(e)(i)-(ii) (disclosure)

An agency may use personal information for a secondary purpose or disclose the information to a third party where the agency believes, on reasonable grounds, that such use or disclosure is necessary:

- to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offenses; or
- for the enforcement of a law that imposes a pecuniary penalty.

SINGAPORE

PDPA, First Schedule, Part 3, paragraph 3

An organization may collect, use, or disclose personal data about an individual where such collection, use, or disclosure is necessary for any investigation relating to a contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law.

VIETNAM

Draft PDP Decree, Article 10(1)(d)

Personal data may be processed without the consent of the data subject where such processing is for the investigation and handling of violations of law.

Necessity for legal proceedings and related purposes

Five of the 14 jurisdictions studied permit processing of personal data without consent where necessary for legal proceedings and/or the related purposes of the administration of justice (**Malaysia**) and provision of legal services (**Singapore**).

RELEVANT PROVISIONS

AUSTRALIA

Privacy Act, APP 6.2(c) read with Section 16A (alternative dispute resolution)

An APP entity may use or disclose personal information for a secondary purpose where such use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

Privacy Act, APP 6.2(e) read with Section 6(1)

An APP entity may use or disclose the information for a secondary purpose if the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for the preparation for, or conduct of, proceedings before any court or tribunal, or the implementation of court/tribunal orders conducted by, or on behalf of, an "***enforcement body***."

Note: "***enforcement body***" covers numerous public authorities tasked with investigating and enforcing crimes and regulatory offenses, including state, territory, and federal police.

HONG KONG SAR

PDPO, Section 60B(b)

Personal data may be used or disclosed for a secondary purpose without the data subject's consent if the use of the data is required in connection with any legal proceedings in Hong Kong SAR.

MALAYSIA

PDPA, Section 6(2)(e)

A data user may process personal data about a data subject if the processing is necessary for the administration of justice.

NEW ZEALAND

Privacy Act, IPP 10(1)(e)(iv) (use for a secondary purpose) and IPP 11(1)(e)(iv) (disclosure)

An agency may use personal information for a secondary purpose or disclose the information to a third party where the use or disclosure is necessary for the conduct of proceedings before any court or tribunal that have been commenced or are reasonably in contemplation.

SINGAPORE

PDPA, First Schedule, Part 3, paragraph 3

An organization may collect, use, or disclose personal data about an individual where the collection, use, or disclosure is necessary for any "***proceedings***" (i.e., any civil, criminal, or administrative proceedings by or before a court, tribunal or regulatory authority) that are related to the allegation of:

- a breach of an agreement;
- a contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or
- a wrong or a breach of a duty for which a remedy is claimed under any law.

PDPA, First Schedule, Part 3, paragraph 5

An organization may collect, use, or disclose personal data about an individual where the collection, use, or disclosure is necessary for the provision of legal services by the organization to another person, or for the organization to obtain legal services.

News reporting in the public interest

Four of the 14 jurisdictions studied permit processing of personal data for the purpose of news reporting in the public interest.

There is significant diversity in the scope and purposes of the relevant provisions.

- The relevant legal basis in **China** is drafted in broad terms and could potentially apply to a wide range of activities and organizations.
- The relevant basis in **Hong Kong SAR** covers the narrow situation of disclosure of personal data to a news provider for a purpose related to news reporting.
- The relevant basis in **Singapore** permits processing of personal data only by a fixed list of legislatively defined news organizations solely for prescribed news activities.
- The relevant basis in **Vietnam** applies to a wide range of organizations but appears designed to constrain the purposes and manner in which personal data may be disclosed in the media.

RELEVANT PROVISIONS

CHINA

PIPL, Article 13(5)

Personal information handlers may handle personal information where such handling is within a reasonable scope to implement news reporting, supervision of public opinion, and other similar activities undertaken in the public interest.

HONG KONG SAR

PDPO, Section 61(2)-(3)

Personal data is exempt from the provisions of DPP 3 in any case in which:

- the use of the data consists of disclosing the data to a data user:
  - whose business, or part of whose business, consists of a "***news activity***;" and
  - solely for the purpose of that activity (or any directly related activity); and
- such disclosure is made by a person who has reasonable grounds to believe, and reasonably believes, that the publishing or broadcasting (wherever and by whatever means) of the data (and whether or not it is published or broadcast) is in the public interest.

"***News activity***" means any journalistic activity and includes the:

- gathering of news for the purpose of dissemination to the public;
- preparation or compiling of articles or programs concerning news for the purpose of dissemination to the public;
- observations on news or current affairs for the purpose of dissemination to the public; or
- dissemination to the public of:
  - any article or program of or concerning news; or
  - observations on news or current affairs.

SINGAPORE

PDPA, First Schedule, Part 2, paragraphs 5 and 6

A "***news organization***" may collect, use, or disclose personal data about an individual without the individual's consent where the collection, use, or disclosure is solely for the news organization's "***news activity***."

"***News activity***" means:

- the gathering of news, or the preparation or compilation of articles or programs of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public; or

- the dissemination to the public or any section of the public of any article or programs of or concerning:
  - news;
  - observations on news; or
  - current affairs.

"***News organization***" means:

- any organization:
  - the business of which consists, in whole or in part, of news activity carried out in relation to a licensable broadcasting service within the meaning of the Broadcasting Act 1994, a newswire service, or the publication of a newspaper; and
  - which, if the organization publishes a newspaper in Singapore which is not exempted from the provisions of Part 3 of the Newspaper and Printing Presses Act 1974, is a newspaper company defined in Section 2(1) of that Act; or
- any organization which provides a broadcasting service in or from Singapore and holds a broadcasting license granted under Section 8 of the Broadcasting Act 1994;

VIETNAM

Draft PDP Decree, Article 6(1)(c)-(d)

Personal data processors and third parties may disclose personal data without the consent of the data subject in the media:

- for the purposes of national defense and security, social order and safety, social ethics, and the health of the community; and
- according to the provisions of the Press Law and in a manner that does not cause economic, honor, spiritual, or material damage to the data subject.

Business transactions

Four of the 14 jurisdictions studied permit processing of personal data without consent for a purpose connected to a sale of, or other transaction concerning, a business entity. This number will increase to 4 of 14 jurisdictions if **India** enacts the Draft PDPB in its current form.

Whereas the relevant provision in **New Zealand** is open-ended and covers any use or disclosure of personal data necessary to facilitate a transaction, the relevant provisions in **Hong Kong SAR** and **Singapore** apply specifically to due diligence exercises in relation to a proposed transaction and permit the parties to whom personal data is disclosed to use or disclose the data only for that purpose.

Further, in both **Hong Kong SAR** and **Singapore**, if the transaction does not proceed or is not completed, then the parties to whom the personal data is disclosed must destroy and/or return the data.

RELEVANT PROVISIONS

HONG KONG SAR

PDPO, Section 63B

Personal data transferred or disclosed by a data user for the purpose of a due diligence exercise to be conducted in connection with a proposed business transaction that involves:

- a transfer of the business or property of, or any shares in, the data user;
- a change in the shareholdings of the data user; or
- an amalgamation of the data user with another body;

is exempt from the provisions of DPP 3 if the following conditions are satisfied:

- the personal data transferred or disclosed must be no more than necessary for the purpose of the due diligence exercise;
- on completion of the proposed business transaction, a party to the transaction or a new body formed as a result of the transaction must offer to the data subject goods, facilities, or services which are the same as or similar to those provided by the data user; and
- it must not be practicable to obtain the prescribed consent of the data subject for the transfer or disclosure.

This exception does not apply if the primary purpose of the proposed business transaction is the transfer, disclosure, or provision for gain of the personal data.

Additionally, if a data user transfers or discloses personal data to a person for the purpose of a due diligence exercise to be conducted in connection with a proposed business transaction described above, the person must:

- only use the data for that purpose; and
- as soon as practicable after the completion of the due diligence exercise:
  - » return the personal data to the data user; and
  - » destroy any record of the personal data that is kept by the person.

INDIA

Draft DPDPB, Section 8(8)(b)

If enacted in its current form, the Draft DPDPB would deem consent to have been given for processing of the data subject's personal data, where such processing is necessary in the public interest, including for mergers, acquisitions, any other similar combinations or corporate restructuring transactions in accordance with the provisions of applicable laws.

NEW ZEALAND

Privacy Act, IPP 11(1)(i)

An agency that holds personal information may disclose such information to any other agency or to any person if the agency believes, on reasonable grounds, that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern.

SINGAPORE

PDPA, PDPA, First Schedule, Part 4

A "***business asset transaction***" refers to:

- the purchase, sale, lease, merger or amalgamation, or any other acquisition, disposal, or financing of:
  - an organization or a portion of an organization;
  - an interest in an organization; or
  - any of the business or assets of an organization, other than any personal data to be disclosed below, as the case may be; and
- includes:
  - the amalgamation of a corporation with one or more related corporations; and
  - the transfer or disposal of any of the business or assets of a corporation to a related corporation;

Where an organization (*X*) is a party or a prospective party to a ***business asset transaction*** with another organization (*Y*) in respect of *Y*'s interest in a third organization (*Z*) (the "**relevant transaction**"), personal data about a contractor, a customer, a director, an employee, an officer, or a shareholder of *Y* ("**applicable individual**") may be:

- collected from *Y* by *X* for the purposes of the ***business asset transaction***;
- is used or disclosed by X in relation to the ***business asset transaction***; or
- is disclosed by *Y* to *X* for the purposes of the business transaction.

Where the business asset transaction concerns any part of *Y* or *Y*'s business assets, the personal data mentioned above must relate directly to that part of *Y* or *Y*'s business assets.

If *X* is a prospective party to the relevant transaction, the following conditions apply:

Where *X* collects the personal data mentioned above from *Y* or *Z*:

- *X* may collect, and *Y* or *Z* may disclose, only personal data that is necessary for *X* to determine whether to proceed with the relevant transaction; and
- *X* and *Y* or *Z* must have entered into an agreement that requires *X* to use or disclose the personal data solely for purposes related to the relevant transaction.

Where Y collects the personal data mentioned above from *Z*:

- *Y* may collect, and *Z* may disclose, only personal data that is necessary for *X* or *Y* to determine whether to proceed with the relevant transaction; and
- *Y* and *Z* must have entered into an agreement that requires *Y* to use or disclose the personal data solely for purposes related to the relevant transaction.
- If *X* enters into the relevant transaction, the following conditions apply:
- *X* may use or disclose the personal data collected from *Y* or *Z* only for the same purposes for which *Y* or *Z* would have been permitted to use or disclose the personal data;
- *Y* may use or disclose the personal data collected from *Z* only for the same purposes for which *Z* would have been permitted to use or disclose the personal data;
- *X*, *Y*, or *Z* must notify the applicable individuals of *Z* whose personal data is disclosed that:
  - the relevant transaction has taken place; and
  - the personal data about them has been disclosed to *X*.

If the relevant transaction does not proceed or is not completed:

- *X* must destroy, or return to *Y* or *Z*, all personal data collected; and
- *Y* must destroy, or return to *Z*, all personal data collected.

Publicly available information

Four of the 14 jurisdictions studied permit processing of personal data without consent if the personal data is publicly available. This number will increase to 4 of 14 jurisdictions if **India** enacts the Draft PDPB in its current form.

Whereas the sole requirement in **Singapore** is that the personal data must be publicly available, the remaining 2 jurisdictions (**China** and **New Zealand**) specify a reasonableness requirement. Additionally, the relevant provision in **China** requires that the personal data was either disclosed by the data subject or otherwise lawfully disclosed.

RELEVANT PROVISIONS

CHINA

PIPL, Article 13(6)

Personal information handlers may handle personal information where the personal information has been disclosed by individuals themselves or has otherwise already been lawfully disclosed, within a reasonable scope according to the provisions of the PIPL.

INDIA

Draft DPDPB, Section 8(8)(f)

If enacted in its current form, the Draft DPDPB would deem consent to have been given for processing of the data subject's personal data, where such processing is necessary in the public interest, including for processing of publicly available personal data.

NEW ZEALAND

Privacy Act, IPP 10(1)(d) (use for a secondary purpose) and IPP 11(1)(d) (disclosure)

An agency may use personal information for a secondary purpose or disclose the information to a third party where the agency believes, on reasonable grounds, that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to use or disclose the information.

SINGAPORE

PDPA, First Schedule, Part 2, paragraph 1

An organization may collect, use, or disclose personal data about an individual where such personal data is publicly available.

Establishing, exercising, or defending a legal right or claim

Three of the 14 jurisdictions studied permit processing of personal data without consent where necessary to establish a legal right or claim.

Whereas the relevant provisions in **Australia** and **Hong Kong SAR** extend also to exercise and defense of such a claim, the relevant provision in **Singapore** focuses instead on establishing the right or claim through investigation and on obtaining legal services.

RELEVANT PROVISIONS

AUSTRALIA

Privacy Act, APP 6.2(c) read with Section 16A

An APP entity may use or disclose the information for a secondary purpose where such use or disclosure is reasonably necessary for the establishment, exercise, or defense of a legal or equitable claim.

HONG KONG SAR

PDPO, Section 60B(c)

Personal data may be used or disclosed for a secondary purpose without the data subject's consent if the use of the data is required for establishing, exercising, or defending legal rights in Hong Kong SAR.

SINGAPORE

PDPA, First Schedule, Part 3, paragraph 3

An organization may collect, use, or disclose personal data about an individual where such collection, use, or disclosure is necessary for any investigation relating to:

- a breach of an agreement;
- a circumstance or conduct that may result in a remedy or relief being available under any law.

PDPA, First Schedule, Part 3, paragraph 5

An organization may collect, use, or disclose personal data about an individual where the collection, use, or disclosure is necessary for the provision of legal services by the organization to another person, or for the organization to obtain legal services.

Cooperating with government agencies

Three of the 14 jurisdictions studied permit processing of personal data without consent where necessary to cooperate with a government agency.

While the relevant provision in **Japan** covers both use and disclosure of personal data for this purpose, the relevant provisions in **India** and **Singapore** apply only to disclosure.

RELEVANT PROVISIONS

JAPAN

APPI, Articles 18(2)(iv) (use for a secondary purpose) and 27(1)(iv) (disclosure)

A business operator handling personal information may handle an individual's personal information beyond the scope necessary to achieve the purpose of use, or disclose an individual's personal information to a third party, without obtaining the individual's prior consent where the handling or disclosure of personal information is necessary for cooperating with a state organ, a local government, or an individual or entity entrusted by either of the former two in executing affairs prescribed by laws and in which obtaining the consent of the individual is likely to impede the execution of such affairs.

SINGAPORE

PDPA, Second Schedule, Part 3, Division 1, paragraph 1 (disclosure)

An organization may disclose personal data about an individual to a ***public agency***, where the disclosure is necessary in the public interest.

A ***public agency*** includes:

- the Government, including any ministry, department, agency, or organ of State;
- any tribunal appointed under any written law; or
- any statutory body established under a public Act for a public function that has been specified by a ministerial notification as a public agency for the purposes of the PDPA.

INDIA

IT Rules, Rule 6 (disclosure)

Prior consent from a provider of SPDI is not required for disclosure of such SPDI by a body corporate to a government agency that has a legal mandate to obtain information (including SPDI) for the purpose of identity verification, or for prevention, detection, investigation, prosecution, and punishment of offenses, including cyber incidents.

The Government agency must send a request in writing to the body corporate possessing the SPDI clearly stating the agency's purpose for seeking such information. The Government agency must also state that information obtained through such a request may not be published or shared with any other person.

Necessity for human resources management

Three of the 14 jurisdictions currently studied permit processing of personal data without consent for purposes related to management of human resources. This number will increase to 3 of 14 jurisdictions if **India** enacts the Draft PDPB in its current form.

RELEVANT PROVISIONS

CHINA

PIPL, Article 13(2)

Personal information handlers may handle personal information where necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts.

INDIA

Draft DPDPB, Section 8(7)

If enacted in its current form, the Draft DPDPB would deem consent to have been given for processing of the data subject's personal data, where such processing is necessary for purposes related to employment, including:

- the prevention of corporate espionage;
- maintenance of confidentiality of trade secrets, intellectual property, and classified information;
- recruitment;
- termination of employment;
- provision of services and/or benefits to data subjects who are employees;
- verification of attendance; and
- assessment of performance.

SINGAPORE

PDPA, First Schedule, Part 3, paragraph 10

An organization may collect, use, or disclose the personal data about an individual where the collection, use, or disclosure is reasonable for the purpose of or in relation to the organization:

- entering into an employment relationship with the individual or appointing the individual to any office; or
- managing or terminating the employment relationship with or appointment of the individual.

Protecting national security

Two of the 14 jurisdictions studied expressly permit processing of personal data in the interests of national security (as opposed to, for example, exempting certain activities or organizations from the application of data protection laws for national security purposes).

Whereas the relevant provision in **Vietnam** permits any such processing that is in the interests of national security, social order, or safety, the provision in **Hong Kong SAR** requires that the processing must be specifically for the purpose of safeguarding such an interest and that obtaining consent would be likely to prejudice these matters.

RELEVANT PROVISIONS

HONG KONG SAR

PDPO, Section 57(2)

Personal data may be used or disclosed for a secondary purpose without the data subject's consent in any case in which:

- the use of the data is for purposes of safeguarding security, defense, or international relations in respect of Hong Kong SAR (and whether or not the data is held for any of those purposes); and
- seeking consent for such use would be likely to prejudice any of these matters.

VIETNAM

Draft PDP Decree, Article 6(1)(b)

Personal data processors and third parties may disclose personal data without the consent of the data subject where the disclosure is necessary for the interests of national security, social order, and safety.

Draft PDP Decree, Article 10(1)(b)

Personal data may be processed without the consent of the data subject for the interests of national security, social order, and safety.

Protecting public revenue

Two of the 14 jurisdictions studied permit processing of personal data without consent where necessary for the protection of public revenue.

RELEVANT PROVISIONS

AUSTRALIA

Privacy Act, APP 6.2(e) read with Section 6(1).

An APP entity may use or disclose personal information for a secondary purpose if the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for protection of public revenue by, or on behalf of, an "***enforcement body***."

The definition of an "***enforcement body***" covers numerous public authorities tasked with investigating and enforcing crimes and regulatory offenses including state, territory, and federal police.

NEW ZEALAND

Privacy Act, IPP 10(1)(e)(iii) (use for a secondary purpose) and IPP 11(1)(e)(iii) (disclosure)

An agency may use personal data for a secondary purpose or disclose the information to a third party where the agency believes, on reasonable grounds, that such use or disclosure is necessary for the protection of public revenue.

Locating missing persons

Australia provides a legal basis that permits processing of personal data without consent for the purpose of locating a person who has been reported missing.

AUSTRALIA

Privacy Act, APP 6.2(c) read with Section 16A

An APP entity may use or disclose personal information for a secondary purpose where:

- the entity reasonably believes that the use or disclosure is reasonably necessary to assist any APP entity, body, or person to locate a person who has been reported as missing; and
- the use or disclosure complies with the rules made by the Commissioner pursuant to Section 16A(2) of the Privacy Act.

Calculating service fees

South Korea provides a legal basis that permits processing of personal data without consent where necessary to calculate service fees. This basis applies only to information and communications service providers.

SOUTH KOREA

PIPA, Article 39-3(2)(2)

An information and communications service provider may collect and use personal information of users without their consent where the information is necessary to calculate fees for the provision of information and communications services.

Business improvement purposes

Singapore provides a legal basis that permits a corporation to obtain personal data from a related corporation and process the data for "business improvement purposes," without obtaining the data subject's consent.

SINGAPORE

"Business improvement purposes" include:

- improving, enhancing, or developing goods and services or methods and processes;
- learning about and understanding the behavior and preferences of individuals in relation to goods and services; and
- identifying goods or services that may be suitable for individuals or personalizing or customizing any such goods or services for individuals.

PDPA, Fifth Schedule

Personal data about an individual (*P*) may be:

- collected by a corporation (*X*) from a related corporation (*Y*) for a ***relevant purpose***;
- used by *X* for a ***relevant purpose***; or
- disclosed by *Y* to *X* for a ***relevant purpose*** subject to the following requirements.

A "***relevant purpose"*** refers to any of the following:

- improving or enhancing any goods or services provided, or developing new goods or services to be provided, by *X* or *Y*;
- improving or enhancing the methods or processes, or developing new methods or processes, for the operations of *X* or *Y*;
- learning about and understanding the behavior and preferences of *P* or another individual in relation to the goods or services provided by *X* or *Y*;
- identifying any goods or services provided by *X* or *Y* that may be suitable for *P* or another individual or personalizing or customizing any such goods or services for *P* or another individual.

Data Sharing from Y to X

Y may disclose *P*'s personal data to *X* (and *X* may collect *P*'s personal data from *Y*) for a ***relevant purpose*** only if:

- the ***relevant purpose*** for which *X* collects, or *Y* discloses, personal data about *P* cannot reasonably be achieved without the collection, use, or disclosure of the personal data in an individually identifiable form;
- a reasonable person would consider the collection or disclosure of personal data about *P* for the ***relevant purpose*** to be appropriate in the circumstances
- *X* and *Y* are bound by any contract or other agreement or binding corporate rules requiring the recipient of personal data about P to implement and maintain appropriate safeguards for the personal data; and
- at the time of the collection or disclosure, *P* is:
  - an ***existing customer*** of *Y*; and
  - an ***existing customer*** or a ***prospective customer of X***.

An ***existing customer*** means an individual who purchases, hires, or uses, or has purchased, hired, or used any goods or services provided by the corporation.

A ***prospective customer of X*** means an individual who, at the time of collection or disclosure:

- has informed *X* of the individual's interest in purchasing, hiring, or using any goods or services provided by *X*; or
- is conducting negotiations with *X* that lead or may lead to an agreement between the individual and *X* for the purchase, hire, or use of any goods or services provided by *X*.

Use of P's the Personal Data

X may only use *P*'s personal data for a ***relevant purpose*** if:

- the ***relevant purpose*** for which X uses personal data about *P* cannot reasonably be achieved without the use of the personal data in an individually identifiable form; and
- a reasonable person would consider the use of personal data about *P* for the ***relevant purpose*** to be appropriate in the circumstances.

Necessity for "evaluative purposes"

Singapore provides a legal basis that permits processing of personal data without consent where necessary for an "evaluative purpose."

SINGAPORE

PDPA, First Schedule, Part 3, paragraph 2

An organization may collect, use, or disclose personal data about an individual where such collection, use, or disclosure is necessary for an "***evaluative purpose***," i.e., the purpose of:

- determining the suitability, eligibility, or qualifications of the individual to whom the data relates for:
  - employment or appointment to office;
  - promotion in employment or office or continuance in employment or office;
  - removal from employment or office;
  - admission to an education institution;
  - the awarding of contracts, awards, bursaries, scholarships, honors, or other similar benefits;
  - selection for an athletic or artistic purpose; or
  - grant of financial or social assistance, or the delivery of appropriate health services, under any scheme administered by a public agency;
- determining whether any contract, award, bursary, scholarship, honor, or other similar benefit should be continued, modified, or canceled;
- deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property; or such other similar purposes as the Minister may prescribe.

Necessity for recovery or payment of a debt

Singapore provides a legal basis that permits processing of personal data without consent where necessary for recovery or payment of a debt

SINGAPORE

PDPA, First Schedule, Part 3, paragraph 4

An organization may collect, use, or disclose personal data about an individual where the collection, use, or disclosure of personal data about an individual is necessary for the organization:

- to recover a debt owed by the individual to the organization; or
- to pay to the individual a debt owed by the organization.

Additionally, if **India**'s Draft DPDPB is enacted in its current form, the Bill would permit a data subject's personal data to be processed without the data subject's consent where necessary for recovery of a debt.

INDIA

Draft DPDPB, Section 8(8)(g)

If enacted in its current form, the Draft DPDPB would deem consent to have been given for processing of the data subject's personal data, where such processing is necessary in the public interest, including for recovery of debt.

Credit reporting

Singapore provides a legal basis that permits processing of personal data without consent where necessary for credit reporting purposes.

SINGAPORE

PDPA, First Schedule, Part 3, paragraph 6(1)

An organization may collect, use, or disclose personal data about an individual where the collection, use, or disclosure:

- is for the purpose of the preparation by a credit bureau of a credit report; or
- relates to a credit report provided by a credit bureau to a member of the credit bureau in relation to a transaction between the member and the individual.

This rule does not apply to a credit bureau that is required to obtain under any other written law but does not hold such a license.

Additionally, if **India**'s Draft DPDPB is enacted in its current form, the Bill would permit a data subject's personal data to be processed without the data subject's consent where necessary for credit scoring.

INDIA

Draft DPDPB, Section 8(8)(d)

If enacted in its current form, the Draft DPDPB would deem consent to have been given for processing of the data subject's personal data, where such processing is necessary in the public interest, including for credit scoring.

Private trust or benefit plan

Singapore provides a legal basis that permits processing of personal data without consent where necessary for a purpose related to a private trust or benefit plan.

SINGAPORE

PDPA, First Schedule, Part 3, paragraph 7
An organization may collect, use, or disclose personal data about an individual where the collection, use or disclosure is to:

- confer an interest or a benefit on the individual under a private trust or benefit plan; and
- administer that trust or benefit plan, at the request of the settlor or the person establishing the benefit plan.

Providing a service for personal or domestic purposes

Singapore provides a legal basis that permits collection of personal data about an individual (*A*) from another individual (*B*), where *B* has provided *A's* personal data to the organization, so that the organization can provide a service to *A* for *A*'s personal or domestic purposes.

SINGAPORE

PDPA, First Schedule, Part 3, paragraph 8
An organization may collect, use, or disclose personal data about an individual where the personal data:

- is provided to the organization by another individual to enable the organization to provide a service for the personal or domestic purposes of that other individual; and
- is collected, used, or disclosed by the organization solely for the purpose of providing a service for the personal or domestic purposes of that other individual.

Document created in course of employment, business, or profession

Singapore provides a legal basis that permits processing of personal data without consent where the personal data is included in a document produced in the course, and for the purposes, of an individual's employment, business, or profession.

SINGAPORE

PDPA, First Schedule, Part 3, paragraph 9
An organization may collect, use, or disclose personal data about an individual where the personal data:

- is included in a document produced in the course, and for the purposes, of the individual's employment, business, or profession; and
- is collected, used, or disclosed for purposes consistent with the purpose for which the document was produced.

LEGITIMATE INTERESTS

This Review has identified that data protection laws in 10 of the 14 jurisdictions studied contain either an express legitimate interest basis for processing personal data without consent or a similar basis that is broadly compatible with a legitimate interest basis.

Data protection laws in 4 jurisdictions (**China**, **India**, **Malaysia**, and **Vietnam**) currently lack such a legitimate interest basis or similar basis.

Importantly, the relevant provisions in the 10 jurisdictions are open-ended and flexible enough that potentially any "legitimate interest" (or equivalent) could be taken into account.

However, there is still considerable divergence in how the relevant provisions are structured and drafted. While this does not preclude all compatibility, it would likely increase compliance costs for businesses that operate across borders and in turn, may hinder adoption of the legitimate interest basis as an alternative to consent.

Recognition of a legitimate interest basis

6 of the jurisdictions studied (**Indonesia**, **Macau SAR**, the **Philippines**, **Singapore, South Korea**, and **Thailand**) have a clearly identifiable "legitimate interest" basis for processing personal data without consent.

5 of these jurisdictions (**Indonesia**, **Macau SAR**, the **Philippines**, **South Korea**, and **Thailand**) have legal bases for processing personal data that resemble the legitimate interest basis in European data protection law, such as the Data Protection Directive,[52] and its successor, the GDPR.

The relevant provisions in **Macau SAR**, the **Philippines**, and **Thailand** most closely resemble the formulation of the legitimate interest basis in the Data Protection Directive. In these jurisdictions, a controller may process a data subject's personal data without obtaining the data subject's consent where the processing is necessary for pursuing the legitimate interests of the controller or a third party, unless such interests are overridden by fundamental rights or freedoms of the data subject (however these rights or freedoms are expressed in each jurisdiction's legal system). To determine whether or not the legitimate interest pursued is overridden by the fundamental rights of the data subject, the controller must undertake a "balancing test" between these two competing considerations.

The relevant provision in **South Korea** has the same core elements as the European formulation but requires a stricter balancing test. Under the PIPA, a controller may collect or use (but not disclose) personal data without obtaining consent where the collection and use is necessary to pursue a legitimate interest of the controller; however, the legitimate interest must "clearly override" the rights of the data subject. The PIPA also imposes additional requirements on top of those in the European formulation: the relevant provision permits processing of personal data on this basis only to the extent that the processing substantially relates to the legitimate interest and is within a reasonable scope.

Indonesia's PDPL contains a legitimate interest provision which shares the same core elements as the European formulation. However, it is unclear how the balancing test should be conducted as the relevant provision only states that the purpose, needs, and the balance of interests between the data controller and the rights of the data subject must be taken into account. This ambiguity may prevent organizations from relying on this basis.

RELEVANT PROVISIONS

INDONESIA

PDPL, Article 20(2)(f)

Personal data may be processed for fulfillment of "other legitimate interests" taking into account the purposes, needs, and balance between the interests of the personal data controller and the rights of the personal data subject.

MACAU SAR

PDPA, Article 6(5).

Personal data may be processed if processing is necessary for pursuing the legitimate interests of the controller or the third party to whom the data is disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms, and guarantees of the data subject.

PHILIPPINES

DPA, Section 12(f)

The processing of personal information is permitted insofar as the personal information is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject that require protection under the Philippine Constitution.

SOUTH KOREA

PIPA, Article 15(1)(6)

A personal information controller may collect personal information and use it with the scope of the purpose of collection where the collection or use is necessary to attain a justifiable interest of the personal information controller, and such interest is manifestly superior to the rights of the data subject.

In such cases, processing is allowed only to the extent the processing is substantially related to the justifiable interest of the personal information controller and does not go beyond a reasonable scope.

THAILAND

PDPA, Section 24(5)

The data controller may collect personal data without the consent of the data subject where such collection is necessary for the legitimate interests of the data controller or any other persons or juristic persons other than the data controller, except where such interests are overridden by the fundamental rights of the data subject of his/her personal data.

Singapore has a unique formulation of the legitimate interest basis, compared with other jurisdictions both in this study and internationally. **Singapore**'s provision is open ended and would allow an organization to rely on potentially any lawful interest of the organization or a third party. However, compared with its European equivalent, the relevant provision in Singapore lacks a necessity requirement and imposes a stricter balancing test: the interest relied upon must "outweigh any adverse effect on the individual."[53] **Singapore**'s provision is also unique in that it requires organizations to undertake a DPIA to identify and implement measures to address any adverse effect to the individual from the processing.

SINGAPORE

PDPA, First Schedule, Part 3

An organization may collect, use, or disclose personal data about an individual where:

- such collection, use, or disclosure is in the legitimate interests of the organization or another person; and
- the legitimate interests of the organization or other person outweigh any adverse effect on the individual.

The organization must:

- conduct an assessment, before collecting, using, or disclosing the personal data to determine whether the above requirements are satisfied; and
- provide the individual with reasonable access to information about the organization's collection, use, or disclosure of personal data in accordance with this provision.

In conducting the assessment, the organization must:

- identify any adverse effect that the proposed collection, use, or disclosure of personal data about an individual is likely to have on the individual;
- identify and implement reasonable measures to:
  - eliminate the adverse effect;
  - reduce the likelihood that the adverse effect will occur; or
  - mitigate the adverse effect; and
- comply with any other prescribed requirements.

Of the 6 jurisdictions that recognize the legitimate interest basis, there is a lack of convergence as to whose interests can be relied on.

- In **Macau SAR**, the **Philippines**, **Singapore**, and **Thailand**, the controller may rely on its own interests or on the interests of a third party. The relevant provisions in **Macau SAR** and the **Philippines** only refer to a third party to whom the personal data has been disclosed. By contrast, the relevant provisions in **Singapore** and **Thailand** are broader and cover any person or corporation other than the controller.
- In **South Korea**, the relevant provision only refers to the interests of the controller. This may prevent a controller from relying on the interests of a third party.
- In **Indonesia**'s PDPL, it is unclear whose legitimate interest the relevant provision refers to.

Recognition of a legal basis that is broadly compatible with the legitimate interest basis

A further 4 jurisdictions (**Australia**, **Hong Kong SAR**, **Japan**, and **New Zealand**) have provisions which share many of the same elements as the legitimate interest basis present in other jurisdictions.

Specifically, in these jurisdictions, consent is not required to collect and use personal data (or in the cases of **Australia** and **Japan**, personal data other than sensitive personal data) for a lawful purpose that is connected with a business's functions or activities. This requirement is similar to the requirement for a legitimate interest in other jurisdictions.

Further, all 4 of these jurisdictions subject collection of personal data to a necessity standard.

- In **Australia** and **New Zealand**, the personal data must be necessary for one or more of the entity's functions or activities.
- In **Hong Kong SAR**, the personal data must be for a lawful purpose that is directly related to a function or activity of the party that will use the data, and the collection must be necessary for or directly related to that purpose.
- In **Japan**, personal data may be handled without the consent of the data subject if the handling is within the scope necessary to achieve the organization's purpose for using the data, which must be clearly defined.

Additionally, all 4 of these jurisdictions subject *collection* of personal data to one or more accountability requirements. **Japan** also imposes an accountability requirement on *use* of personal data.

While these requirements are less comprehensive than the "balancing test" required in the European formulation of the legitimate interest basis or the detailed requirement to conduct an impact assessment in **Singapore**'s formulation, they typically involve some, but not all, of the same considerations, such as lawfulness and fairness of the means of collection, and, in the case of **Hong Kong SAR**, the extent of data collection. **New Zealand**'s requirements come closest to a balancing test by expressly requiring the entity to consider the impact of collection on data subjects' personal affairs.

However, jurisdictions in this category differ from jurisdictions which expressly recognize a legitimate interest basis in terms of the interests that may be relied upon. For jurisdictions in this category, it is unclear whether an entity could rely on the interests of a third party as the majority of these jurisdictions require that the collection of personal data must relate to a function or activity of the entity itself and/or that the collection must be necessary to achieve that entity's legitimate business purpose.

RELEVANT PROVISIONS

AUSTRALIA

Privacy Act, APP 3.2
An APP entity must not collect personal information (other than sensitive personal information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Privacy Act, APP 3.5
An APP entity must collect personal information only by lawful and fair means.

Privacy Act, APP 6.1

If an APP entity holds personal information about an individual that was collected for a particular purpose (the ***primary purpose***), the entity must not use or disclose the information for another purpose (the ***secondary purpose***) unless:

- the individual has consented to the use or disclosure of the information; or
- an exception under APP 6.2 applies in relation to the use or disclosure of the personal information about the individual.

HONG KONG SAR

PDPO, DPP 1(1)
Personal data may not be collected unless:

- the data is collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
- the collection of the data is necessary for or directly related to that purpose; and
- the data is adequate but not excessive in relation to that purpose.

PDPO, DPP 1(2)
Personal data must be collected by means that are lawful and fair in the circumstances of the case.

PDPO, DPP 3
Personal data must not, without the prescribed consent of the data subject, be used for any purpose other than the purpose for which the data was to be used at the time of the collection of the data or a purpose directly related to thereto.

Note: The term "use," in relation to personal data, includes disclosure or transfer of the data (PDPO, Section 2(1)).

JAPAN

APPI, Article 17
When handling personal information, a business operator handling personal information must specify the purpose of use as clearly as possible.

APPI, Article 18(1)
A business operator handling personal information must not handle personal information beyond the scope necessary to achieve the purpose of use without the prior consent of the person.

APPI, Article 19
business operators handling personal information must not use personal information in any way that may contribute to or induce illegal or unjust conduct.

APPI, Article 20
Business operators handling personal information must not acquire personal information through deception or other wrongful means.

NEW ZEALAND

Privacy Act, IPP 1(1)
An agency must not collect personal information unless:

- the information is collected for a lawful purpose connected with a function or an activity of the agency; and
- the collection of the information is necessary for that purpose.

Privacy Act, IPP 4
An agency may collect personal information only by a means that:

- is lawful; and
- in the circumstances of the case:
  - is fair; and
  - does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

No equivalent to the legitimate interest basis

The remaining 4 jurisdictions studied (**China**, **India** (IT Rules), **Malaysia**, and **Vietnam**) lack a legitimate interest basis or equivalent.

China

Of these jurisdictions, **China** comes closest to having equivalent structures to legitimate interest in its data protection law.

China has legal bases for processing personal data which cover purposes that would likely be recognized as legitimate interests in other jurisdictions, such as news reporting and human resources management.

It also is possible that further purposes could be added via the catch-all provision for "processing provided in law and administrative regulations" in Article 13(7) of the PIPL. Combined with other provisions in the PIPL, this would bring **China**'s data protection law very close to having a legitimate interest basis as the other elements for such a basis are arguably already present in the PIPL.

Specifically, it may be possible to read the requirements for a legitimate interest or purpose, and necessity, into the principles of legality and necessity in Article 5 of the PIPL. Further, Articles 55 and 56 already require a "balancing test" of sorts as a personal information handler must consider whether processing may have a major influence on individuals; if so, the personal information handler would specifically have to undertake a DPIA taking into account similar factors as those considered in the legitimate interest test, including:

- whether the purpose and methods for processing the personal information are lawful, legitimate, and necessary;
- the possible impact of the processing on the data subject's rights and interests; and
- whether protective measures undertaken are legal, effective, and suitable to the degree of risk.

CHINA

PIPL, Article 5

The principles of legality, propriety, necessity, and sincerity must be observed for personal information handling. It is prohibited to handle personal information in misleading, swindling, coercive, or other such ways.

PIPL, Article 13(7)

Personal information handlers may handle personal information where laws and administrative regulations provide other circumstances in which handling of personal information is permitted.

PIPL, Article 55

Personal information handlers must conduct a personal information protection impact assessment in advance, and record the handling situation, where personal information handling activities have a major influence on individuals.

PIPL, Article 56

The content of the personal information protection impact assessment must include:

- whether or not the personal information handling purpose and handling method, etc., are lawful, legitimate, and necessary;
- the influence on individuals' rights and interests, and the security risks; and
- whether protective measures undertaken are legal, effective, and suitable to the degree of risk.

Personal information protection impact assessment reports and handling status records must be preserved for at least three years.

India

Although **India**'s IT rules do not provide for a legitimate interest basis (or equivalent) for processing personal data, the Draft DPDPB, if enacted in its current form, would provide a similar legal basis to the legitimate interest basis. However, the relevant provision does not appear to be as open-ended as equivalents in other jurisdictions. Rather, the wording of this provisions suggests that organizations would only be able to rely on the provision to process personal data for purposes prescribed in regulation. It is also unclear whether the provision requires organizations, or the regulator, would to apply the balancing test.

INDIA

Draft DPDPB, Section 8(9)

If enacted in its current form, the Draft DPDPB would deem consent to have been given for processing of the data subject's personal data, where such processing is necessary for any fair and reasonable purpose as may be prescribed after taking into consideration:

- whether the legitimate interests of the data fiduciary in processing for that purpose outweigh any adverse effect on the rights of the data subject;
- any public interest in processing for that purpose; and
- the reasonable expectations of the data subject, having regard to the context of the processing.

COLLECTIVE BENEFITS OF LEGAL CERTAINTY AND CONVERGENCE

While there are many potential areas for convergence or interoperability of data protection laws in Asia-Pacific, the comparisons presented in this Review indicate that there are also divergences. This lack of interoperability may create legal uncertainty, compliance challenges for organizations that operate in multiple jurisdictions, and could exacerbate well documented risks for both data subjects and businesses, such as the problem of "consent fatigue."[54]

Despite differences in cultural norms and variations in regulatory models, Asia-Pacific jurisdictions share a mutual interest in bridging gaps between their respective data protection frameworks. Efforts towards convergence will have a positive impact on organizations, individuals, and regulators by enhancing legal certainty and facilitating compliance.

1. A unified set of legal bases for processing personal data across multiple Asia-Pacific jurisdictions would help organizations that operate across borders to comply with multiple legal frameworks.

Having common legal bases for processing personal data without consent across Asia-Pacific would facilitate cross-border compliance as organizations would be able to implement common solutions for each category of data in each jurisdiction, avoiding unnecessary duplication of compliance efforts. This is important for small and medium enterprises and start-ups who lack the capabilities of large multinational companies for dealing with complex regulations.

2. Removing legal uncertainty, gaps between laws, and complexity in cross-border compliance with data protection laws is in the interest of individuals.

Variations in data protection frameworks across Asia-Pacific may impede the effective cross-border implementation of individuals' data protection rights and may also limit capacities for effective regulatory oversight once personal data leaves a given jurisdiction. Additionally, multiplying compliance efforts across jurisdictions constrains organizations' internal privacy resources, which could otherwise be used to improve substantive data protection practices to benefit individuals. This includes the operational costs of planning in the face of regulatory uncertainty and of adapting business and compliance functions and transactional structures.

3. Compatible legal frameworks help the community of data protection authorities to cooperate and share insights, experiences, and approaches to implementation.

Greater coherence between and harmonization of regional legal frameworks, particularly relating to legal bases for processing personal data, would help to create the necessary common ground for regulatory cooperation and exchange of ideas, facilitating consistent regulatory action.

4. Consistency with global standards benefits all stakeholders.

Considering the integration of Asia-Pacific economies in global trade and the increasing privacy expectations of the Asia-Pacific public, consistency between sub-regional, regional, and global frameworks helps to reduce the layers of complexity that currently hinder cross-jurisdictional compliance and regulatory cooperation.

REBALANCING CONSENT AND PRIVACY ACCOUNTABILITY IN ASIA-PACIFIC: A ROADMAP

Several jurisdictions both in Asia-Pacific and globally have already undertaken, or are in the process of undertaking, comprehensive reviews of their data protection laws to reposition consent and promote accountability-focused alternatives. The experiences of these jurisdictions can provide a useful model for other jurisdictions that are considering similar reforms to their data protection laws. This Section of the Review will therefore outline the main reforms undertaken in each of these jurisdictions, identify measures that have been successfully implemented, and present a "toolkit" of measures that other jurisdictions could consider adopting when reforming their data protection laws.

Review of efforts to rebalance notice and consent internationally

Canada

In 2015, Canada introduced a new provision into the Personal Information Protection and Electronic Documents Act ("**PIPEDA**") conditioning the validity of an individual's consent on whether it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose, and consequences of the collection, use, or disclosure of the personal information to which they are consenting.

CANADA

PIPEDA, Schedule 1, clause 4.3
The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

PIPEDA, Section 6.1
For the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

Further, in 2016, the Office of the Privacy Commissioner of Canada ("**OPC**") launched a public consultation on the issue of consent under the PIPEDA.[55]

In May 2016, the OPC published a Discussion Paper identifying issues with the current consent model in the PIPEDA and soliciting feedback on possible changes.[56]

The OPC received 51 written submissions in response to the Discussion Paper[57] and held several roundtables and focus group discussions to seek feedback from stakeholders and members of the Canadian public.[58] Common themes across many of the submissions include the need for more detailed guidance on consent requirements in the PIPEDA and privacy-enhancing measures like de-identification. The submissions also identified several systemic issues with consent and possible policy improvements including the need to simplify or standardize privacy policies and consider technical solutions to privacy, the possibility of designating "no-go zones" (i.e., uses of personal data that would be prohibited even if consent for such use is obtained), and ethical assessments, especially in the context of new and emerging technologies.[59]

In its Annual Report to Parliament on the PIPEDA ("**Annual Report**") the following year, the OPC outlined several measures based on feedback received from stakeholders during the public consultation. While the OPC recognized the need for mechanisms beyond consent to increase privacy protection, the OPC's proposed reforms focused primarily on consent as the OPC took the view that consent, if given meaningfully and with better information, could still play an important role in protecting privacy. Notably, the OPC also highlighted the importance of extra-legal solutions, such as Privacy by Design and Privacy by Default approaches.

Making consent meaningful

In 2018, the OPC released its "**Guidelines for obtaining meaningful consent**"[60] integrating feedback from the public consultation. These Guidelines (which were revised in 2021) emphasize that consent should remain central to protection of personal data but would need to be made meaningful again as technological advances and modern practices had made consent illusory.

Canada's PIPEDA recognizes both express and implied forms of consent. The OPC's 2018 "Guidelines for obtaining meaningful consent" provide guidance on when each form of consent is appropriate.

In particular, the Guidelines recommend that express consent should be required where:

- the personal data in question is sensitive;
- data subjects would not reasonably expect the processing of their data in the circumstances; and/or
- the processing creates a meaningful residual risk of significant harm.

Where any of the above factors is not present, the OPC permits organizations to rely on implied consent.

Sensitivity

Unlike many data protection laws in Asia-Pacific, Canada's PIPEDA does not specify certain categories of personal data as "sensitive." Rather, sensitivity of personal data is a factor to be taken into consideration in all processing of personal data and is context specific, reflecting a **risk-based approach**. For example, clause 4.3.4 of Schedule 1 to the PIPEDA provides an example that although the names and addresses of subscribers to a news magazine generally would not be considered sensitive, the names and addresses of subscribers to certain special-interest magazines might be considered sensitive.

The Guidelines recognize that in practice, certain categories of personal data would generally be considered sensitive because processing of these categories of personal data brings specific risks to individuals. However, the Guidelines clarify that whether personal data qualifies as sensitive depends on the circumstances.

For example, the Guidelines explain that seemingly benign information may become sensitive if it can reveal sensitive data when combined with other information. Conversely, personal data that would generally be considered sensitive may become less sensitive if that information is already in the public domain, depending on the purpose for which such information is being made public and the nature of the relationship between the parties involved.

Risk of harm

The Guidelines consider that under the principle of accountability in the PIPEDA, an organization would be required to implement measures to mitigate any risks identified in the processing of an individual's personal data. The Guidelines recognize that in some cases, such measures may significantly reduce the risks but in other cases, there may still be residual risks.

The Guidelines therefore advise that if there is a meaningful residual risk of significant harm, the organization should notify individuals of this risk and obtain their express consent before processing their personal data.

According to the Guidelines, a risk is "meaningful" if there is more than a minimal possibility that the risk will materialize. Additionally, "significant harm" refers to bodily harm, humiliation, damage to reputation or relationships, loss of employment, loss of business or professional opportunities, financial loss, identity theft, negative effects on credit records, and damage to or loss of property. The Guidelines take a broad view of harm that includes not only harms arising directly from the processing of personal data but also reasonably foreseeable harms caused by third parties.

Singapore

Singapore has taken the lead in Asia in providing alternatives to consent.

Singapore's Personal Data Protection Act 2012 ("**PDPA**"), since it was enacted in November 2012, had made consent a central requirement for collecting, using, or disclosing personal data.

However, in 2017 the Personal Data Protection Commissioner of Singapore ("**PDPC**") commenced a public consultation on approaches to manage personal data in the digital economy.[61] This consultation culminated in a series of substantial amendments to the PDPA in 2020, which, among others, introduced into the PDPA a variation of the legitimate interest basis for processing personal data.

In a paper published by the PDPC in July 2017 ("**PDPC Consultation Paper**"), the PDPC identified several challenges to consent in the digital economy, including:

- passive collection and analysis of large amounts of personal data, making it harder for individuals to anticipate the purposes of processing and for businesses to identify and obtain consent from every individual whose data is collected and processed;
- information overload;
- consent fatigue;
- lack of informed consent;
- consent not appropriate for all purposes, including broader societal good from detection of fraud and security threats; and
- need for organizational accountability and responsible data use, but also innovation.[62]

To address these challenges, the PDPC considered it necessary to introduce several new alternatives legal bases to consent for processing personal data into the PDPA[63] and through the PDPC Consultation Paper sought feedback on, among others, proposals for two new legal bases for processing personal data, premised on notification[64] and on a "legal or business purpose,"[65] respectively (see below).

In response to the PDPC Consultation Paper, the PDPC received 68 submissions from individuals and organizations spanning industry, the legal sector, and academia.[66]

In February 2018, the PDPC published its "Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy" ("**PDPC Response Paper**").[67] Broadly, the submissions supported the PDPC's proposals for the two new legal bases but raised issues with certain requirements, prompting PDPC to clarify or otherwise modify its proposals (see below).

The revised proposals in the PDPC's Response Paper culminated in a Bill to amend the PDPA. The Bill brought substantial changes to the original framework, introducing, among others, a new provision on "deemed consent by notification," as well as new exceptions to consent for "legitimate interests" and "business improvement" purposes.

A further public consultation on the draft Bill took place in May 2020,[68] during which time the PDPC received 87 submissions from industry, the legal sector, academia, and individuals.[69]

The amendment Bill was passed in 2020. At the time, Singapore's government explained that the amendments were motivated by the digital economy and a desire to strike a balance between the interests of individuals (e.g., confidence that their data will be secure and used responsibly in the digital economy) and organizations (e.g., legal certainty around use data for legitimate business purposes, subject to safeguards and accountability).[70]

Legitimate interests

In the 2017 PDPC Consultation Paper, the PDPC explained that although Singapore's data protection framework permitted organizations to process personal data for certain specified "legal or business purposes" (such as for an investigation, legal proceedings, recovery of a debt, or research), the PDPC recognized that there may be other circumstances where organizations might need to process personal data without consent for a legitimate purpose, but where such processing would not be authorized under Singapore's existing data protection law.[71]

The PDPC therefore proposed to introduce a general legal basis that would permit organizations to process personal data without consent where:

- the processing is necessary for a "legal or business purpose;"
- it is not desirable or appropriate to obtain consent; and
- the benefits to the public (or a section thereof) clearly outweigh any adverse impact or risks to the data subject, subject to measures to identify and minimize risks to the data subject, such as a risk impact assessment.[72]

In the subsequent PDPC Response Paper, the PDPC reframed this proposal as a "legitimate interest" basis (drawing a clearer link to European data protection law) and clarified that their intent was to enable organizations to process personal data without consent in circumstances where there is a need to protect legitimate interests that will have economic, social, security, or other benefits for the public.[73] In response to feedback received during the public consultation, the PDPC also proposed removing the condition that the legal basis could only be relied upon in situations where it is not desirable or appropriate to obtain consent.[74]

Following the public consultation, the First Schedule of the PDPA was amended in 2020 to include a new "legitimate interests" provision as follows:

SINGAPORE

PDPA, First Schedule, Part 3

An organization may collect, use, or disclose personal data about an individual where:

- such collection, use, or disclosure is in the legitimate interests of the organization or another person; and
- the legitimate interests of the organization or other person outweigh any adverse effect on the individual.

The organization must:

- conduct an assessment, before collecting, using, or disclosing the personal data (as the case may be), to determine whether the above requirements are satisfied; and
- provide the individual with reasonable access to information about the organization's collection, use or disclosure of personal data (as the case may be) in accordance with this provision.

In conducting the assessment, the organization must:

- identify any adverse effect that the proposed collection, use, or disclosure (as the case may be) of personal data about an individual is likely to have on the individual;
- identify and implement reasonable measures to:
  - eliminate the adverse effect;
  - reduce the likelihood that the adverse effect will occur; or
  - mitigate the adverse effect; and
- comply with any other prescribed requirements.

Deemed consent

Deemed consent by conduct

Since the PDPA was first enacted in 2012, the PDPA has permitted organizations to rely on "deemed consent by conduct"[75] for collection, use, or disclosure of an individual's personal data where the individual, without giving actual consent (whether express or implied), voluntarily provides personal data to an organization for a specific purpose, and it is reasonable that the individual would do so.

SINGAPORE

PDPA, Section 15

An individual is deemed to consent to the collection, use, or disclosure of personal data about the individual by an organization for a purpose if:

- the individual, without actually giving consent mentioned in Section 14 of the PDPA, voluntarily provides the personal data to the organization for that purpose; and
- it is reasonable that the individual would voluntarily provide the data.

If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organization to another organization for a particular purpose, the individual is deemed to consent to the collection, use, or disclosure of the personal data for that particular purpose by that other organization.

Deemed consent by contractual necessity

Unlike other data protection laws in the region, the PDPA, prior to the 2020 amendments, did not provide an exception to consent requirements, or a distinct legal basis, for performance of a contract between an individual and an organization.

A proposal to introduce a new form of "deemed consent by contractual necessity" was included in the May 2020 public consultation on the Bill to amend the PDPA. An accompanying document released by the Ministry of Communication and Information ("**MCI**") and the PDPC explained that this proposed provision would deem consent to have been given for the disclosure of personal data to, and the use of the personal data by, third-party organizations where reasonably necessary for the conclusion or performance of a contract or transaction between an individual and an organization.[76]

The 2020 amendments to the PDPA added a new provision to Section 15 of the PDPA on "deemed consent by contractual necessity."[77] This provision serves a similar function to exceptions and legal bases for performance of a contract in other data protection laws.

SINGAPORE

PDPA, Section 15

An individual (*P*) who provides personal data to an organization (*A*) with a view to *P* entering into a contract with *A* is deemed to consent to the following where reasonably necessary for the conclusion of the contract between *P* and *A*:

- the disclosure of that personal data by A to another organization (B);
- the collection and use of that personal data by B; and
- the disclosure of that personal data by *B* to another organization (*C*).

Where *C* collects personal data disclosed to *C* by *B* pursuant to the above provision, *P* is deemed to consent to:

- the collection and use of that personal data by C; and
- the disclosure of that personal data by *C* to yet another organization.

Without limiting the above provisions, an individual (*P*) who enters into a contract with an organization (*A*) and provides personal data to *A* pursuant or in relation to that contract is deemed to consent to the following:

- the disclosure of that personal data by *A* to another organization (*B*), where the disclosure is reasonably necessary for either of the following purposes ("**relevant purpose**"):
  - for the performance of the contract between *P* and *A*; or
  - for the conclusion or performance of a contract between *A* and *B* which is entered into at *P*'s request, or which a reasonable person would consider to be in *P*'s interest;
- the collection and use of that personal data by *B*, where the collection and use are reasonably necessary for a relevant purpose; and
- the disclosure of that personal data by *B* to another organization (*C*), where the disclosure is reasonably necessary for a relevant purpose.

Where *C* collects personal data disclosed to *C* by *B* pursuant to the above provision, *P* is deemed to consent to:

- the collection and use of that personal data by *C*, where the collection and use are reasonably necessary for a relevant purpose; and
- the disclosure of that personal data by *C* to yet another organization, where the disclosure is reasonably necessary for a relevant purpose.

These subsections do not affect any obligation under the contract between *P* and *A* that specifies or restricts:

- the personal data provided by P that A may disclose to another organization; or
- the purposes for which A may disclose the personal data provided by P to another organization.

Deemed consent by notification

During the 2017 public consultation on proposed amendments to the PDPA, the PDPC — drawing comparison with data protection laws in Australia, British Columbia, Japan, and New Zealand — proposed introducing a new provision into the PDPA that would permit organizations to process personal data where:

- the organization notifies the data subject of the purpose for processing the data subject's personal data;
- it is feasible for the organization to allow individuals to opt out of the processing;
- it is impractical for the organization to obtain consent; and
- the processing is not expected to have any adverse impact on the data subject.[78]

This provision appears to have been intended to address:

- situations in which an organization does not have the contact information of its customers but wishes to use its customers' personal data for a secondary purpose of conducting analytics to develop new products and services; and
- deployment of IoT sensor devices and drones, leading to instantaneous collection of large amounts of personal data, where there is no foreseeable impact to data subjects from processing of their personal data in these situations.[79]

In response to feedback, the PDPC opted to reframe this proposed provision as a form of deemed consent and clarified that it would not be possible to rely on the provision for direct marketing purposes.[80]

The 2020 amendments to the PDPA introduced a new provision on "deemed consent by notification," which provides a legal basis to collect, use, or disclose an individual's personal data, subject to a risk impact assessment.

SINGAPORE

PDPA, Section 15A

An individual is deemed to consent to the collection, use, or disclosure of personal data about the individual by an organization if:

- before collecting, using, or disclosing any personal data about the individual, the organization;
  - » conducts an assessment to determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual; and
  - » takes reasonable steps to bring the following information to the attention of the individual:
    - the organization's intention to collect, use or disclose the personal data;
    - the purpose for which the personal data will be collected, used, or disclosed;
    - a reasonable period within which, and a reasonable manner by which, the individual may notify the organization that the individual does not consent to the organization's proposed collection, use or disclosure of the personal data; and
- the individual does not notify the organization, before the expiry of the reasonable period mentioned above, that the individual does not consent to the proposed collection, use or disclosure of the personal data by the organization.

Further requirements for the assessment are found in Section 15A(5) of the PDPA and Regulations 14 and 15 of the PDP Regulations.

Note: This provision cannot be relied upon for any of the following purposes:

- offering to supply goods or services;
- advertising or promoting goods or services;
- advertising or promoting a supplier, or prospective supplier, of goods or services;
- offering to supply land or an interest in land;
- advertising or promoting land or an interest in land;
- advertising or promoting a supplier, or prospective supplier, of land or an interest in land;
- offering to provide a business opportunity or an investment opportunity;
- advertising or promoting a business opportunity or an investment opportunity; or
- advertising or promoting a provider, or prospective provider, of a business opportunity or an investment opportunity.

Business improvement purposes

Plans for the business improvement provision were first introduced in the May 2020 public consultation on the Bill to amend the PDPA.

An accompanying document released by the MCI and the PDPC explained that this proposed provision would permit processing of personal data without consent for the following purposes:

- operational efficiency and service improvements;
- developing or enhancing products/services; and
- knowing the organization's customers.[81]

The document added that this provision was intended to provide clarity for organizations and permit them to harness personal data for these purposes.[82]

SINGAPORE

PDPA, Fifth Schedule
Personal data about an individual (*P*) may be:

- collected by a corporation (*X*) from a related corporation (*Y*) for a ***relevant purpose***;
- used by *X* for a ***relevant purpose***; or
- disclosed by *Y* to *X* for a ***relevant purpose***

subject to the following requirements.

A ***relevant purpose*** refers to any of the following:

- improving or enhancing any goods or services provided, or developing new goods or services to be provided, by *X* or *Y*;
- improving or enhancing the methods or processes, or developing new methods or processes, for the operations of *X* or *Y*;
- learning about and understanding the behavior and preferences of *P* or another individual in relation to the goods or services provided by *X* or *Y*;
- identifying any goods or services provided by *X* or *Y* that may be suitable for *P* or another individual or personalizing or customizing any such goods or services for *P* or another individual.

Data Sharing from Y to X

Y may disclose *P*'s personal data to *X* (and *X* may collect *P*'s data from *Y*) for a ***relevant purpose*** only if:

- the ***relevant purpose*** for which *X* collects, or *Y* discloses, personal data about *P* cannot reasonably be achieved without the collection, use, or disclosure of the personal data in an individually identifiable form;
- a reasonable person would consider the collection or disclosure of personal data about *P* for the ***relevant purpose*** to be appropriate in the circumstances
- *X* and *Y* are bound by any contract or other agreement or binding corporate rules requiring the recipient of personal data about P to implement and maintain appropriate safeguards for the personal data; and
- at the time of the collection or disclosure, *P* is:
  - an ***existing customer*** of *Y*; and
  - an ***existing customer*** or a ***prospective customer of X***.

An ***existing customer*** means an individual who purchases, hires, or uses, or has purchased, hired, or used any goods or services provided by the corporation.

A ***prospective customer of X*** means an individual who, at the time of collection or disclosure:

- has informed *X* of the individual's interest in purchasing, hiring, or using any goods or services provided by *X*; or
- is conducting negotiations with *X* that lead or may lead to an agreement between the individual and *X* for the purchase, hire, or use of any goods or services provided by *X*.

Use of P's Personal Data

X may only use *P*'s personal data for a ***relevant purpose*** if:

- the ***relevant purpose*** for which X uses personal data about *P* cannot reasonably be achieved without the use of the personal data in an individually identifiable form; and
- a reasonable person would consider the use of personal data about *P* for the ***relevant purpose*** to be appropriate in the circumstances.

Australia

Though consent has not traditionally played as large a role in Australia's data protection law as in the data protection laws of other jurisdictions in this Section,[83] a recent review of Australia's Privacy Act has raised issues of consent and the need to promote greater accountability of organizations.

Background

In recent years, Australian authorities have been contemplating a massive overhaul of the Privacy Act to better regulate the digital economy and large digital platforms that have a major impact on the private lives of Australian citizens.

The process began in June 2019 with the Australian Competition and Consumer Commission ("**ACCC**")'s publication of a detailed "Digital Platforms Inquiry" report ("**DPI Report**"), which made recommendations on issues relating to privacy as well as competition and consumer protection in digital markets.[84]

In response to the DPI Report, Australia's Federal Government committed to initiate a review of the Privacy Act and begin consultation on options for implementing several of its privacy-specific recommendations to better empower consumers, protect their data, and support the digital economy.

In October 2020, the Attorney General's Department ("**AGD**") commenced the public consultation by publishing a "Privacy Act Review Issues Paper" ("**AGD Issues Paper**").[85]

A year later, in October 2021, the AGD published a "Privacy Act Review Discussion Paper" ("**AGD Discussion Paper**")[86] outlining more detailed proposals for reform, based on over 200 submissions that the AGD received in response to the AGD Issues Paper.[87]

Consent

In the DPI Report, the ACCC recommended strengthening consent requirements in the Privacy Act, so that the Privacy Act would, by default, require consent to be obtained for any processing of personal data through a clear affirmative act that is freely given, specific, unambiguous, and informed.[88]

However, the DPI Report also acknowledged the issue of "consent fatigue" and recommended implementing measures to address this issue.[89] To reduce consent fatigue, the ACCC recommended requiring consent when personal data is used for an extraneous or unexpected purpose, drawing a distinction between a map app using GPS location data to provide directions and using the same data for targeted advertising.[90] Notably, the ACCC recognized that consent has become an increasingly complex and burdensome task for consumers in the digital economy and that obtaining consent may not provide sufficient protection of personal data.[91]

By contrast, the AGD noted in the AGD Discussion Paper that submitters "overwhelmingly opposed" giving consent a more prominent role in the Privacy Act and considered that although consent may be necessary in certain situations, consent should not be relied upon frequently.[92]

The AGD expressly acknowledged submitters' concerns regarding:

- "consent fatigue;"
- the burdensome nature of consent requirements:
  - for businesses, especially where individuals do not want or need to consent, or where individuals or the broader community would reasonably expect personal data to be processed for a particular purpose; and
  - for individuals, who are expected to understand and consider complex data practices and identify possible harms; and
- the lack of meaningful consent in modern data practices.[93]

The AGD Discussion Paper therefore made a more modest recommendation that the Privacy Act should be amended to include a more detailed definition of consent that would require consent to be voluntary, informed, current, specific, and unambiguous through clear action.[94] These proposed conditions are based on existing guidance issued by the Office of the Australian Information Commissioner ("**OAIC**")[95] and are similar to the conditions for valid consent in the GDPR.

The AGD also considered limiting the role of consent to processing of personal data which poses the highest privacy risk for individuals, and processing of personal data for secondary purposes.[96]

Legitimate interests

In the DPI Report, the ACCC considered a proposal to adopt the legitimate interest basis for processing personal data found in European data protection law, including the GDPR, but ultimately recommended against adopting this basis in the Privacy Act, citing perceived uncertainty in the legitimate interest basis given the broad and flexible definition of a "legitimate interest."[97]

The AGD Discussion Paper notes that 20 submitters spanning industry, academia, civil society, and the privacy community, including the OAIC and the Law Council of Australia, recommended adopting the legitimate interest basis for processing personal data.[98]

The AGD considered this proposal but ultimately opted to recommend a general requirement that entities do not undertake acts or practices in relation to an individual's personal information that would be unfair, cause harm, or be outside the reasonable expectations of an ordinary individual.[99]

However, the distinction may only be academic as in practice, if Australia adopted a reasonableness requirement, its requirements for processing personal data would be similar to those under the legitimate interest basis. In particular, the Privacy Act would permit processing of personal data without consent for a wide variety of purposes that are necessary for organizations' functions or activities, subject to an impact assessment and consideration of the reasonable expectations of data subjects.

Summary of Recommendations

1. Consent should be retained as one of several legal bases for processing personal data. However, consent requirements should be implemented consistently across Asia-Pacific jurisdictions, and regulators and data protection authorities should promote consistency in guidance around the circumstances where consent is appropriate. Regulators and data protection authorities in Asia-Pacific would also benefit from recognizing a "spectrum" of valid consent, covering express opt-in consent, implied opt-in consent, and opt-out consent.
2. Existing alternatives to consent in data protection laws should be retained but, in some cases, may benefit from greater clarity.
3. Regulators and data protection authorities in Asia-Pacific could consider promoting a legitimate interest basis for processing personal data (or equivalent) to future-proof data protection laws and provide a flexible alternative to consent, especially for situations where consent is inappropriate.

The current notice and consent model can only be rebalanced if laws and guidelines are updated to provide complementary provisions to consent, including alternative legal bases.

This section of the Review therefore provides a "toolkit" of measures, drawn from successful attempts to rebalance the consent model around the world, that jurisdictions in Asia-Pacific could consider to increase organizational accountability and reduce the burden of privacy self-management on individuals.

Though legal reform may be required to implement these recommendations, the comparative analysis undertaken for this Review indicates that most of the jurisdictions studied already have structures in their data protection laws, regulations, and guidelines that could support it, and many of the measures proposed in this section of the Review could be achieved if data protection authorities in Asia-Pacific issue consistent guidelines in key areas.

There may also be a need for regulatory incentives, mechanisms, and guidance to support these alternatives and enable organizations to demonstrate compliance effectively and change existing business practices comfortably. Additionally, there is room for solutions outside of the regulatory space, such as technical solutions like Privacy by Design and Privacy-Enhancing Technologies, to play an important role.

Consent

Consent requirements are the area most in need of convergence and consistency in Asia-Pacific data protection laws. Although all 14 of the jurisdictions studied in this Review recognize consent as a legal basis for processing personal data, there is no consistent definition of consent or common set of conditions for valid consent across these jurisdictions. In fact, no single condition for consent is shared by all jurisdictions equally.

This has a number of negative consequences: data subjects across Asia-Pacific would not enjoy a consistent standard of data protection from one jurisdiction to the next, and for businesses that operate in multiple jurisdictions, the costs and complexity of compliance would increase. However, the need for legal reform also creates an opportunity to rethink the role and position of consent as a legal basis for processing

personal data in data protection frameworks in Asia-Pacific, with a view to addressing the difficulties in how consent is used in practice today in a way that will re-establish the balance between the interests of organization, individuals, and the digital economy.

In this regard, regulators in Asia-Pacific can learn from the experiences of jurisdictions that have sought to reform the role of consent in their respective data protection laws in recent years. Notably, none of those jurisdictions have proposed to do away with consent. Rather, the focus of reform has been on repositioning the role of consent in the data protection framework, identifying situations in which it makes the most sense for organizations to rely on consent and providing alternatives to consent for situations in which it does not make sense to rely on consent.

This Review therefore recommends that data protection laws should retain consent as a legal basis for processing personal data, including transferring personal data across borders, but make consent meaningful again, by:

- returning consent to the position it held in the earliest data protection frameworks (such as the OECD Guidelines, the Data Protection Directive, and the data protection laws of Australia, Hong Kong SAR, and New Zealand) as one element among many; and
- ensuring that consent requirements are implemented consistently across Asia-Pacific jurisdictions.

Consent requirements in law should be principle- and outcome-based. Regulators in Asia-Pacific could work together to agree on a common set of guidelines for consent, focusing in particular on two related areas:

- the situations in which it makes sense for organizations to rely on consent; and
- the forms that valid consent may take.

Whereas the legitimate interests basis covers low-risk processing of personal data and processing where there are interests which take precedence over the data subject's autonomy (e.g., where processing is reasonably expected or is not relevant to the data subject, or where data subject may not consent to the processing, but there are important reasons why the personal data should be processed), there may still be situations where the legitimate interest basis is inappropriate or unavailable and where data subjects ought to be given the opportunity to make a meaningful decision about whether to permit processing of their personal data. Here, consent still has an important role to play as a mechanism to give effect to data subjects' autonomy.

As this Review has already discussed, data subjects' autonomy is an important consideration but is not the sole consideration in all processing of personal data. One of the main issues with consent requirements (especially requirements for express, opt-in consent) today is that they can be burdensome for both individuals and organizations without guaranteeing greater protection. For individuals, this can lead to "consent fatigue" which can render consent less meaningful.

One way to reduce the burden of consent on individuals and organizations would be to calibrate the level of consent required to the risk of processing. Following the 2020 amendments to Singapore's PDPA, Singapore's data protection law now recognizes a spectrum of valid consent from a spectrum from authorization to, in some cases, acquiescence:

- express opt-in consent, where the data subject is informed of, and expressly agrees to, a specific kind of processing;
- implied opt-in consent, where a data subject agrees to a specific kind of processing, but this agreement can be inferred from the data subject's words or conduct;
- opt-out consent, where a data subject is given a reasonable opportunity to opt out of a specific kind of processing within a specific timeframe and is deemed to consent to the processing if the data subject does not opt out within that timeframe.

Similarly, in Canada (whose PIPEDA recognizes both express and implied forms of consent), the OPC — following a public consultation on reforming the role of consent in the PIPEDA — issued guidance that express consent would generally only be required for:

- sensitive processing of personal data (this is broader than, but would overlap with, processing of legislatively defined classes of sensitive personal data);
- processing that the data subject would not reasonably expect; and
- processing of personal data that presents a high risk of significant harm to the data subject.

Regulators in Asia-Pacific could consider expressly recognizing that valid consent can take different forms involving different levels of response from data subjects.

The strictest consent requirements would likely only be necessary in a minority of situations like those identified in Canadian guidelines. In these situations, it would be most appropriate to require consent to be express, voluntary, informed, current, specific, and unambiguous. As these requirements already align with existing requirements for valid consent in the majority of jurisdictions studied, this reform could be achieved if relevant authorities across the Asia-Pacific region issued a consistent set of guidelines.

It may not be necessary to impose such strict requirements for valid consent in other situations where, for example, data subjects would expect their personal data to be processed for a specific purpose and would obviously give consent if asked.

For example, Singapore's PDPC provides a useful example of a scenario where consent can be "deemed" from the circumstances and the actions of the data subject.

SINGAPORE

PDPA Key Concepts Guidelines, Paragraph 12.23 (Example)

Sarah makes a visit to a spa for a facial treatment. After the treatment is completed, she makes her way to the cashier to make payment. The cashier tells her that the facial will cost her $49.99. She hands over her credit card to the cashier for the purpose of making payment. The cashier need not ask for Sarah's consent to collect, use or disclose her credit card number and any other related personal data (e.g., name on credit card) required to process the payment transaction. Sarah would be deemed to have consented to the collection, use and disclosure of her credit card number and other related personal data for processing of the payment as she voluntarily provided the personal data and it is reasonable that Sarah would provide the personal data to pay for her facial. Sarah's deemed consent would extend to all other parties involved in the payment processing chain who collect or use Sarah's personal data. These parties could include, for example, Sarah's bank, the spa's bank and its processers and the payment system provider.

Notably, **India**'s Draft DPDPB, released for public consultation in November 2022, has adopted a similar concept of deemed consent. If enacted in its current form, Section 8(1) of the Draft DPDPB would permit consent for processing of a data subject's personal data to be deemed if the data subject voluntarily provides personal data to an organization for a specific purpose, and it is reasonable to expect that the data subject would do so.

INDIA

Draft DPDPB, Section 8(1) (Illustration)

'A' shares her name and mobile number with a Data Fiduciary for the purpose of reserving a table at a restaurant. 'A' shall be deemed to have given her consent to the collection of her name and mobile number by the Data Fiduciary for the purpose of confirming the reservation.

Permitting organizations to rely on forms of consent involving lower levels of response from data subjects, such as implied or deemed consent, where appropriate would remove some of the burden of giving consent for individuals in situations where it is not necessary. Of course, such consent should only be recognized for a limited range of purposes for which the data subject's expectation and agreement are obvious — in the above example, completing the transaction. It would not be appropriate to extend the implied consent to processing for a secondary purpose, such as direct marketing. To process personal data for a secondary purpose, the organization would have to rely on an alternative legal basis, such as legitimate interests (where appropriate) or seek consent.

Realigning Consent Requirements in Asia-Pacific

A barrier to convergence is that at present, only a minority of jurisdictions in Asia-Pacific expressly recognize different forms of valid consent, such as express and implied consent.

In other jurisdictions, data protection authorities have either expressly rejected implied consent, or there is a definition of consent in the data protection law that appears to prevent organizations from relying on implied consent. Legal reform would be required in these jurisdictions to fully realize the above proposals.

Balancing Legal Certainty and Flexibility in Consent Requirements

Broadly, jurisdictions in Asia-Pacific could benefit from consistency in the conditions for consent and the circumstances in which the strictest forms of consent should apply. However, a barrier to convergence in some jurisdictions is a lack of flexibility in how relevant provisions are drafted.

In most jurisdictions studied, conditions for consent are found in guidelines issued by the data protection authority, rather than in legislation. This allows for greater flexibility as it enables data protection authorities to update requirements for valid consent without the need for full legal reform.

However, for jurisdictions whose laws specify the requirements for valid consent, an option to consider is to move towards more open-ended provisions in law and combine these with detailed guidance from the data protection authority or regulator. Fixed lists give the appearance of legal certainty and may be perceived to facilitate compliance by giving businesses a list of boxes to check. However, in practice, such requirements can limit the ability of the data protection authority (which may be closest to the issues) to update the data protection framework in response to new situations and challenges.

As for specific areas which would benefit from convergence, regulators and data protection authorities in this region could consider issuing a consistent set of guidelines around informed consent, and the procedure for, and effect of, withdrawing consent for processing of personal data.

In particular, this Review has revealed that while a significant portion of jurisdictions studied require that consent must be informed, there is ambiguity as to the information that must be provided, and how requirements for informed consent interact with notification requirements (especially considering that notification requirements may be subject to exceptions). Jurisdictions in Asia-Pacific would benefit from clarity as to how requirements for informed consent interact with separate requirements to notify the data subject of data collection.

Alternative legal basis to consent

An important step towards reducing the burden of privacy self-management on individuals is to ensure that data protection laws provide viable alternative lawful grounds to process personal data, other than consent.

Limitations of Existing Alternaives

This Review has shown that all jurisdictions studied provide alternative legal bases to consent for processing personal data in at least certain circumstances, such as in emergencies, or for performance of a contract or compliance with a legal obligation.

These existing alternatives are important and necessary as they cover situations where it would be inappropriate or infeasible to require organizations to obtain consent — for example, where:

- there is a need to protect or give effect to an interest that supersedes the need to give effect to the data subject's autonomy (such as protecting a person from harm or complying with a legal obligation), especially where consent cannot be easily obtained in an appropriate timeframe (such as in a health emergency); or
- obtaining further consent is unnecessary because the data subject's intentions are clear (such as where processing of personal data is necessary to perform an obligation under a contract with the data subject or fulfill a request from the data subject during precontractual negotiations).

To that end, this Review recommends that where data protection laws contain legal bases that permit personal data to be processed without consent, these legal bases should be retained, though clarity and convergence may still be needed.

However, the usefulness of these existing legal bases for shifting compliance practices away from consent may be limited for two main reasons:

- Firstly, these bases cover only a fixed list of situations and are often, by design, very narrow in scope, dealing with specific situations like emergencies and compliance with legal or contractual obligations.
- Secondly, the jurisdictions studied diverge significantly in the number and type of alternative legal bases to consent that each jurisdiction recognizes. Many alternative legal bases identified in this Review are unique to a single jurisdiction and do not have equivalents in other jurisdictions, even if there are sound policy reasons for permitting processing of personal data without consent on those bases.

Legitimate Interests

Compared with other alternatives legal bases to consent, a flexible alternative legal basis exists in data protection law in a number of jurisdictions globally, including Asia-Pacific.

This legal basis has been expressed in several different ways: "legitimate interests," "reasonable purposes," and "legitimate business purposes." However, fundamentally, these formulations all share the same core requirements:

- a lawful purpose for processing; and

- an impact assessment, which either takes the form of a "balancing test" between the interests of the organization (or a third party) and the rights and interests of the data subject, or a data protection impact assessment.

Some jurisdictions also expressly require that the processing must be necessary and/or that the organization must consider the reasonable expectations of the data subject.

The strength of the legitimate interest basis is that it can be as flexible as consent. Unlike other alternative legal bases to consent, the legitimate interest basis is not limited to specific purposes or situations; rather, it is open-ended and can be used to legitimize potentially any legitimate purpose for processing personal data in a wide range of different situations, provided that the above requirements are satisfied.

However, compared with consent, the legitimate interest basis shifts the onus of privacy management onto the organizations that seek to process personal data by effectively requiring such organizations to "self-regulate" rather than requiring data subjects to "self-manage" their privacy.[100] Specifically, organizations seeking to rely on the legitimate interest basis must:

- be able to identify and describe a specific legitimate interest that would justify the processing of the data subject's personal data without consent; and
- prove that they have considered the impact of processing on the data subject and, where necessary, have implemented measures to mitigate any potential risks.

Recognition of the Legitimate Interests Basis Globally

EU

The legitimate interest basis is well-established in the EU and was present in the EU's first comprehensive data protection law, commonly known as the Data Protection Directive, which was passed in 1995.

EU

Data Protection Directive, Article 7(1)(f)

Personal data may be processed if processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1) [i.e., the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.]

The Data Protection Directive was replaced by the GDPR, which was passed in 2016 and took effect in 2018.[101] However, GDPR retained the "legitimate interests" provision in largely the same form as that of the Data Protection Directive, with minor amendments (underlined).

EU

GDPR, Article 6(1)(f)

Processing of personal data is lawful if and to the extent that the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Under European law, an entity seeking to rely on this legal basis must be able to demonstrate that three distinct requirements are met:[102]

- **Purpose:** The processing of personal data must be in pursuit of a "legitimate interest" of the data controller or a third party.
- **Necessity:** The processing must be necessary for the purpose of pursuing the legitimate interest.
- **Balance of interests:** The entity must weigh the purpose for processing against the data subject's rights and freedoms and demonstrate that the data subject's rights and freedoms do not override the purpose for processing. If such rights and freedoms override the purpose for processing, processing will not be lawful. The balancing exercise should also take into account the reasonable expectations of data subjects, based on their relationship with the entity.

Brazil

The legitimate interest basis has also been adopted in Brazil.[103]

BRAZIL

Law Nº 13,709/18 (as amended by Law No. 13,853/2019), Article 7(9)
The processing of personal data may be conducted when necessary to meet the legitimate interests of the controller or third party, except in the event that the fundamental rights and freedoms of the holder that require the protection of personal data prevail.

Law Nº 13,709/18 (as amended by Law No. 13,853/2019), Article 10
The legitimate interest of the controller may only justify processing of personal data for legitimate purposes, considered from concrete situations, which include, but are not limited to:

- support and promotion of the controller's activities; and
- protection of the regular exercise of the data subject's rights or provision of services that benefit the data subject, respecting the data subject's legitimate expectations and fundamental rights and liberties, pursuant to the terms of this Law.

When processing is based on the legitimate interest of the controller, only personal data that is strictly necessary for the purpose intended may be processed.

The controller must adopt measures to ensure the transparency of data processing based on its legitimate interest.

The national authority may request the controller to provide a personal data protection impact report, when the processing is based on its legitimate interest, subject to commercial and industrial confidentiality.

Asia

Most recently, **Singapore** has taken the lead in moving away from a consent-centric model through its 2020 amendments to the PDPA, which introduced a variation of the legitimate interest basis that incorporates an express requirement for a data protection impact assessment.

Additionally, **India**'s draft Personal Data Protection Bill — which was tabled in the lower house of India's Parliament in December 2019 but ultimately withdrawn in August 2022 — contained a similar provision, which would have permitted processing of personal data without consent where necessary for a "reasonable purpose" that would have been specified in regulations.[104]

Developing Legitimate Interests in Asia-Pacific

In practice, it is expected that the legitimate interest basis would cover most routine forms of processing conducted by businesses that:

- are of low impact to data subjects;
- data subjects would reasonably expect; and/or
- serve an interest that takes precedence over data subjects' autonomy (e.g., fraud detection, cybersecurity), subject to the balancing test.

Unless there is a good reason not to do so, data subjects could be notified that their data is processed on this basis for a specific purpose.

This Review has revealed that most jurisdictions studied either expressly recognize legitimate interests as a legal basis for processing personal data or have a legal basis that permits processing of personal data without consent, if organizations comply with conditions that are broadly similar to those for the legitimate interest basis.

The minority of jurisdictions that do not currently recognize legitimate interests as a basis for processing personal data could consider adding this legal basis in future law reform.

Guidance

Of the 6 jurisdictions that currently recognize a legitimate interest basis, 4 jurisdictions (**Macau SAR**,[105] the **Philippines**[106] **Singapore**,[107] and **South Korea**[108]) have issued some form of guidance, whether in the form of guidelines from the data protection authority, case notes, or advisory opinions, on how organizations may rely on this basis.

All 4 of these jurisdictions give some indication of interests that would likely be recognized as legitimate. However, only guidelines in the **Philippines** and **Singapore** provide information on how to conduct the balancing exercise/impact assessment.

Compatibility between these jurisdictions' data protection laws could be greatly increased if regional regulators cooperate on a set of common guidelines on how organizations operating in Asia-Pacific could rely on this legal basis, especially in relation to:

- the "use cases" in which this legal basis could apply; and
- how the balancing exercise/impact assessment should be conducted.

This coordination would, in turn, build organizations' confidence in using the legal basis, especially for cross-border compliance.

Future guidelines can take inspiration from existing guidance in Asia-Pacific, as well as established global precedents like those from the EU, as this is the jurisdiction with the longest experience with the legitimate interest basis. An instructive guide, referred to below, is the "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" (**Opinion 06/2014**) by a Data Protection Working Party set up under Article 29 of the Data Protection Directive, which has since been superseded by the GDPR.[109] Though this Opinion interprets Article 7 of the Directive, it remains relevant to Article 6(1)(f) of the GDPR, which is substantially similar (see above).

Use cases

It is not possible or desirable to identify all possible use cases for the legitimate interest basis, as the strength of this basis lies in its flexibility. While a body of use cases will eventually emerge on a case-by-case basis, regulators and data protection authorities in Asia-Pacific could increase compatibility of the legitimate interest basis across their respective jurisdictions by collaborating on a common set of regional guidelines recommending general categories of interests that would generally be recognized as legitimate and would usually fall within reasonable expectations of data subjects.

As a starting point, Opinion 06/2014 provides a non-exhaustive list of possible use cases, including:

- exercise of the right to freedom of expression or information, including in the media and the arts;
- conventional direct marketing and other forms of marketing or advertisement;
- unsolicited non-commercial messages, including for political campaigns or charitable fundraising;
- enforcement of legal claims including debt collection via out-of-court procedures;
- prevention of fraud, misuse of services, or money laundering;
- employee monitoring for safety or management purposes;
- whistle-blowing schemes;
- physical security, IT, and network security;
- processing for historical, scientific, or statistical purposes; and
- processing for research purposes (including marketing research).[110]

Additionally, regulators and data protection authorities could look globally to the experiences of other jurisdictions that have already implemented a legitimate interest basis for processing personal data, including the EU[111] and Brazil,[112] to further develop these general categories.

Impact assessment

Regulators can also offer guidance as to how the assessment should be undertaken and documented, accepting that the assessment will depend on contextual factors.

Many jurisdictions have issued guidelines on how organizations should undertake the necessary assessment to rely on the legitimate interest basis. These jurisdictions include:

- the EU (pre-GDPR);[113]
- the United Kingdom[114] (whose guidance has been adopted in the Philippines[115]); and
- Singapore.[116]

Generally, factors relevant to the assessment include:

The legitimate interest or purpose for processing, including:

- whether interest is lawful, specific enough that the balancing test can be conducted, and real and present, rather than merely speculative;
- whether the processing of personal data is necessary to achieve the interest pursued;
- whether there are other less invasive means to achieve purpose of the processing; and
- the reasonableness of the purpose for processing the personal data.

The benefits to the organization, the data subject, the public (whether the whole or a segment of the public) and/or specific sectors or industries from the processing, including any potential harms to any of these parties if the personal data is not processed.

The nature of the personal data to be processed, including its sensitivity.

The impact of the processing on the data subject, including:

- the rights and/or interests of the data subject that could be impacted;
- the likely impact of the processing on the data subject, including any reasonably foreseeable harms to the data subject (e.g., financial, social, physical, psychological effects), and the likelihood and severity of those effects; and
- whether information from other data sets will be used to make predictions or decisions involving the data subject, and if so, whether these predictions or decisions exclude, discriminate against, defame, or harm the data subject.

The relationship between the organization and the data subject, including relative bargaining power, and the reasonable expectation of the data subject.

The nature of the processing, including:

- the types of personal data that will be processed for this purpose;
- the manner in which the personal data will be processed; and
- whether the processing is on a large scale or involves data mining, profiling, disclosure to a large number of people, or publication; and
- whether the personal data will be processed on a one-off or continuous basis.

Any measures that the organization can adopt to mitigate, eliminate, or reduce risks of harm, including:

- data minimization;
- technical and organizational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals;
- anonymization and pseudonymization;
- Privacy Enhancing Technologies and Privacy by Design techniques;
- data protection impact assessments;
- increased transparency; and
- a right to object or opt-out of processing.

Any residual harms that are likely to remain after the above measures have been implemented.

Transparency, including whether data subjects have been informed that their personal data may be processed on the basis of a legitimate interest, or whether the organization has made available the contact information of a person who can provide the data subject with further information on how their personal data will be processed.

ENDNOTES

* The Future of Privacy Forum is grateful to Dr Clarisse Girot for her significant contributions to the development of this Review.

1 ABLI, "Convergence of data privacy laws and frameworks for cross-border transfers of personal data in Asia," available at https://abli.asia/Projects/Data-Privacy-Project

2 ABLI, "Transferring Personal Data in Asia: A path to legal certainty and regional convergence" (May 2020), available at https://payhip.com/b/BT1P

3 Daniel Solove, "Privacy Self-Management and the Consent Dilemma." Harvard Law Review 126 (2013): 1880-1903

4 FPF, "Joint Project to Explore Limits of Consent In Asia-Pacific Data Privacy Regimes" (September 3, 2021), available at https://fpf.org/press-releases/joint-project-to-explore-limits-of-consent-in-asia-pacific-data-privacy-regimes/

5 Clarisse Girot, Katerina Demetzou, Sebastião Barros Valle, and Rob Van Eijk, "Event Report: From "Consent-Centric" Frameworks to Responsible Data Practices and Privacy Accountability In Asia Pacific" (September 28, 2021), available at https://fpf.org/blog/event-report-from-consent-centric-frameworks-to-responsible-data-practices-and-privacy-accountability-in-asia-pacific/

6 Aashish Aryan, "Government releases Digital Personal Data Protection Bill draft" *Economic Times* (November 19, 2022), available at https://economictimes.indiatimes.com/tech/technology/government-releases-digital-personal-data-protection-bill-draft/articleshow/95599120.cms

7 Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A Free and Fair Digital Economy – Protecting Privacy, Empowering Indians," pages 32-42, available at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

8 John Edwards, "Click to consent? Not good enough anymore" (September 2, 2019), available at https://www.privacy.org.nz/blog/click-to-consent-not-good-enough-anymore/

9 Caroline Hopland, Hunter Dorwart, and Gabriela Zanfir-Fortuna, "Singapore's Personal Data Protection Act Shifts Away from a Consent-Centric Framework" (November 18, 2020), available at https://fpf.org/blog/singapores-personal-data-protection-act-shifts-away-from-a-consent-centric-framework/

10 Australian Government Attorney General's Department ("**AGD**"), "Review of the Privacy Act 1988," available at https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988

11 Personal Data Protection Commissioner, Ministry of Communications and Multimedia Malaysia, "Public Consultation Paper No. 01/2020, Review of Personal Data Protection Act 2010 (Act 709)," page 6, available at https://www.pdp.gov.my/jpdpv2/assets/2020/02/Public-Consultation-Paper-on-Review-of-Act-709_V4.pdf

12 Andy Yu and Dora Si, "China Data Privacy Update – Enhanced Scrutiny of "Bundled Consent,"" (April 30, 2021), available at https://www.deacons.com/news-and-insights/publications/china-data-privacy-update-%E2%80%93-enhanced-scrutiny-of-%E2%80%9Cbundled-consent%E2%80%9D.html

13 Jasmine Park, "South Korean Personal Information Protection Commission Announces Three-Year Data Protection Policy Plan" (December 22, 2020), available at https://fpf.org/blog/south-korean-personal-information-protection-commission-announces-three-year-data-protection-policy-plan/

14 Ministry of Justice, "Broadening the Privacy Act's notification rules" (August 24, 2022), available at https://www.justice.govt.nz/justice-sector-policy/key-initiatives/broadening-the-privacy-acts-notification-rules/

15 Available at https://fpf.org/tag/apac-jurisdiction-report-series/

16 Available at https://www.legislation.gov.au/Details/C2022C00199

17 Available at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines

18 An English translation is available at https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

19 An English translation is available at https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf

20 Available at https://www.elegislation.gov.hk/hk/cap486

21 Available at https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

22 Available at https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf

23 Available in Indonesian at https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20220920-123712-3183.pdf. Note that this version of the Bill was released after publication of the Jurisdiction Report on the Status of Consent for Processing Personal Data in Indonesia in July 2022.

24 Available in Japanese at https://elaws.e-gov.go.jp/document?lawid=415AC0000000057

25 Available in Japanese at https://elaws.e-gov.go.jp/document?lawid=415CO0000000507

26 Available in Japanese at https://www.ppc.go.jp/files/pdf/211116_guidelines01.pdf

27 Available in Japanese at https://www.ppc.go.jp/files/pdf/2205_APPI_QA.pdf

28 An English translation is available at https://www.gpdp.gov.mo/file/Laws%20and%20Regulations/%E5%80%8B%E4%BA%BA%E8%B3%87%E6%96%99%E4%BF%9D%E8%AD%B7%E6%B3%95_EN.pdf

29 Available at https://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf

30 Available at https://www.pdp.gov.my/jpdpv2/assets/2019/09/Peraturan-peraturan_Perlindungan_Data_Peribadi.pdf

31 Available at https://www.legislation.govt.nz/act/public/2020/0031/latest/whole.html#whole

32 Available at https://www.privacy.gov.ph/data-privacy-act/

33 Available at https://www.privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/

34 Available at https://www.privacy.gov.ph/advisory-opinions/

35 Available at https://sso.agc.gov.sg/Act/PDPA2012?WholeDoc=1

36 Available at https://sso.agc.gov.sg/SL/PDPA2012-S63-2021?WholeDoc=1

37 Available at https://www.pdpc.gov.sg/guidelines-and-consultation/2020/03/advisory-guidelines-on-key-concepts-in-the-personal-data-protection-act

38 An English translation is available at https://elaw.klri.re.kr/kor_service/lawView.do?hseq=53044&lang=ENG

39 An English translation is available at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=54521&lang=ENG

40 Guidelines and Commentary on the Personal Information Protection Act ("**PIPA Guidelines**"), pages 91-94, available in Korean at https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS061&mCode=C010010000&nttId=6969#LINK

41 An English translation is available at https://www.mdes.go.th/uploads/tinymce/source/%E0%B8%AA%E0%B8%84%E0%B8%AA/Personal%20Data%20Protection%20Act%202019.pdf
42 Available in Thai at https://www.doe.go.th/prd/assets/upload/files/hrad_th/5ae086c0cc7414c7861efe2d0cf48a68.pdf
43 Available on the website of Thailand's Ministry of Digital Economy and Society. Note that these guidelines were issued after publication of ABLI and FPF's Jurisdiction Report on the Status of Consent for Processing Personal Data in Thailand in August 2022.
44 Available in Vietnamese at http://bocongan.gov.vn/vanban/Pages/van-ban-moi.aspx?ItemID=418.
45 APPI Q&A, Question 1-61 (page 16).
46 See ABLI and FPF's Jurisdiction Report on the Status of Consent for Processing Personal Data in Japan, section 5.1(b), available at https://fpf.org/blog/new-report-on-limits-of-consent-in-japans-data-protection-law/
47 Available at https://www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-007.pdf
48 Security Specification, paragraph 3.
49 See ABLI and FPF's Jurisdiction Report on the Status of Consent for Processing Personal Data in Malaysia, section 5.1, available at https://fpf.org/blog/new-report-on-limits-of-consent-in-malaysias-data-protection-law/
50 See ABLI and FPF's Jurisdiction Report on the Status of Consent for Processing Personal Data in New Zealand, section 8, available at https://fpf.org/blog/new-report-on-limits-of-consent-in-new-zealands-data-protection-law/
51 See ABLI and FPF's Jurisdiction Report on the Status of Consent for Processing Personal Data in Japan, above n 44, section 5.2; ABLI and FPF's Jurisdiction Report on the Status of Consent for Processing Personal Data in Macau SAR (August 2022), pages 8-9, available at https://fpf.org/blog/new-report-on-limits-of-consent-in-macaus-data-protection-law/; and ABLI and FPF's Jurisdiction Report on Consent for Processing Personal Data in New Zealand, above, section 4.2.
52 Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 ("**Data Protection Directive**").
53 This standard is similar to that in Article 15(1)(6) of South Korea's PIPA.
54 Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, Thorsten Holz, "(Un)informed Consent: Studying GDPR Consent Notices in the Field", 2019, available at https://arxiv.org/abs/1909.02638
55 Office of the Privacy Commissioner of Canada ("**OPC**"), "Notice of consultation on consent under the PIPEDA" (July 27, 2016), available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-consent-under-pipeda/consent_notice-avis_201605/
56 OPC, "A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act" (May 2016), available at https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/.
57 The OPC has also published all submissions received during the 2016 public consultation on consent on its website, available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-consent-under-pipeda/submissions-received-for-the-consultation-on-consent/
58 https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-consent-under-pipeda/
59 *Ibid*.
60 OPC, "Guidelines for obtaining meaningful consent" (August 13, 2021), available at https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/
61 Personal Data Protection Commission of Singapore ("**PDPC**"), "Public Consultation for Approaches to Managing Personal Data in the Digital Economy," available at https://www.pdpc.gov.sg/guidelines-and-consultation/2017/07/public-consultation-for-approaches-to-managing-personal-data-in-the-digital-economy
62 PDPC, "Public Consultation for Approaches to Managing Personal data in the Digital Economy" (July 27, 2017) ("**PDPC Consultation Paper**"), pages 4-5, available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/publicconsultationapproachestomanagingpersonaldatainthedigitaleconomy270717f95e65c8844062038829ff000.ashx?la=en
63 *Ibid,* page 5.
64 *Ibid,* pages 6-8.
65 *Ibid,* pages 8-10.
66 The responses to the public consultation are published on the PDPC's website at https://www.pdpc.gov.sg/Guidelines-and-Consultation/2017/07/Public-Consultation-for-Approaches-to-Managing-Personal-Data-in-the-Digital-Economy/Responses-Received-on-5-October-2017
67 PDPC, "Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy" (February 1, 2018) ("**PDPC Response Paper**"), available at PDPC-Response-to-Feedback-for-Public-Consultation-on-Approaches-to-Managing-Personal-Data-in-the-Dig.ashx
68 Ministry of Communications and Information, Singapore ("**MCI**"), "Public Consultation on the Draft Personal Data Protection (Amendment) Bill" (May 28, 2020), available at https://www.mci.gov.sg/public-consultations/public-consultation-items/public-consultation-on-the-draft-personal-data-protection-amendment-bill
69 MCI, "Responses received from Public Consultation on draft Personal Data Protection (Amendment) Bill 2020, including related amendments to the Spam Control Act" (June 6, 2020), available at https://www.mci.gov.sg/public-consultations/public-consultation-items/responses-on-draft-personal-data-protection-amendment-bill
70 Opening Speech by Minister for Communications and Information, S. Iswaran, at the Second Reading of the Personal Data Protection (Amendment) Bill 2020 on November 2, 2020, available at https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/11/opening-speech-by-minister-iswaran-at-the-second-reading-of-pdp-(amendment)-bill-2020
71 PDPC Consultation Paper, pages 8-9.
72 *Ibid,* page 9.
73 PDPC Response Paper, pages 7-8.
74 *Ibid,* page 8-9.
75 Advisory Guidelines on Key Concepts in the Personal Data Protection Act ("**PDPA Key Concepts Guidelines**"), page 42, available at https://www.pdpc.gov.sg/guidelines-and-consultation/2020/03/advisory-guidelines-on-key-concepts-in-the-personal-data-protection-act
76 MCI, "Public Consultation Paper Issued by the Ministry of Communications and Information and the Personal Data Protection Commission Draft Personal Data Protection (Amendment) Bill, including Related Amendments To The Spam Control Act" (May 14, 2020) ("**PDPA Amendment Bill Consultation Paper"**), page 12, available at https://www.mci.gov.sg/-/media/MciCorp/Doc/Public-Consultations/Public-Consultation-on-PDP-Amendment-Bill---14May2020/PDP-Amendment-Bill.ashx

77 PDPA Key Concepts Guidelines, page 44.
78 PDPC Consultation Paper, pages 6-7.
79 *Ibid*, page 7; Issues Paper, pages 4-5.
80 PDPC Response Paper, page 6.
81 PDPA Amendment Bill Consultation Paper, page 13.
82 *Ibid*.
83 ABLI-FPF Jurisdiction Report on the Status for Processing Personal Data in Australia, available at https://fpf.org/blog/new-report-on-limits-of-consent-in-australias-data-protection-law/
84 ACCC, "Digital Platforms Inquiry Final Report" (June 2019) ("**DPI Report**"), available at https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf
85 AGD, "Privacy Act Review Issues Paper" (October 2020), available at https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-cth-issues-paper
86 AGD, "Privacy Act Review Discussion Paper" (October 2021) ("**AGD Discussion Paper**"), available at https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/
87 The AGD has also published all submissions received in response to the AGD Discussion Paper on its website, available at https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/published_select_respondent
88 DPI Report, pages 35 and 464-470.
89 *Ibid*, page 489.
90 *Ibid*, page 470.
91 *Ibid*.
92 AGD Discussion Paper, pages 75-76.
93 *Ibid*, page 75.
94 *Ibid*, pages 11 and 77-78.
95 Office of the Australian Privacy Commissioner ("**OAIC**"), "Australian Privacy Principles Guidelines" (July 2019, paragraph B.37, available at https://www.oaic.gov.au/__data/assets/pdf_file/0009/1125/app-guidelines-july-2019.pdf
96 AGD Discussion Paper, page 76.
97 *Ibid*, pages 466 and 489.
98 DPI Report, page 83.
99 *Ibid*, page 83.
100 Charmian Aw and Cynthia O'Donoghue, "Processing Personal Data Based on Legitimate Interests: A Paradigm Shift" [2019] PDP Digest, page 76, available at https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/2019-personal-data-protection-digest.ashx
101 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**GDPR**").
102 United Kingdom Information Commissioner's Office ("**ICO**"), "What is the 'legitimate interests' basis?" available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/
103 Available in Portuguese at http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm
104 Personal Data Protection Bill, 2018 (India), s 14, available at https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
105 Macau SAR's data protection authority has released case notes for several cases in which a legitimate interest was identified: see ABLI and FPF's Jurisdiction Report on the Status of Consent for Processing Personal Data in Macau SAR (August 2022), pages 8-9, available at https://fpf.org/blog/new-report-on-limits-of-consent-in-macaus-data-protection-law/
106 The Philippines' data protection has issued a number of advisory opinions on the legitimate interest basis: see ABLI and FPF's Jurisdiction Report the Status of Consent for Processing Personal Data in the Philippines (July 2022), pages 11-12, available at https://fpf.org/blog/new-report-on-limits-of-consent-in-the-philippines-data-protection-law/
107 PDPA Key Concepts Guidelines, above, paragraph 12.62 and Annex C.
108 Guidelines and Commentary on the Personal Information Protection Act ("**PIPA Guidelines**"), pages 91-94, available in Korean at https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS061&mCode=C010010000&nttId=6969#LINK
109 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (April 9, 2014) ("**Opinion 06/14**"). Note that following enactment of the GDPR, the Article 29 Working Party has since been replaced by the European Data Protection Board ("**EDPB**").
110 *Ibid*, page 25.
111 FPF and Nymity, "Processing Personal Data on the Basis of Legitimate Interests under the GDPR: Practical Cases," available at https://fpf.org/wp-content/uploads/2018/04/20180413-Legitimate-Interest_FPF_Nymity-2018.pdf
112 For a detailed compilation of use cases for the legitimate interest basis in Brazil, see Bruno Ricardo Bioni, Mariana Rielli, and Marina Kitayama, "Legitimate Interests Under the Brazilian General Data Protection Law: General Framework and Concrete Examples," available at https://www.observatorioprivacidade.com.br/wp-content/uploads/2021/05/LI-under-LGPD_Data-Privacy-Brasil-Research-Association.pdf
113 Opinion 06/2014, page 55.
114 *Supra*, n 102.
115 *Supra*, n 106.
116 PDPC Key Concepts Guidelines, Annex C.

The Asian Business Law Institute (ABLI) is a permanent think tank based in Singapore that initiates, conducts and facilitates research with a view to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

1 SUPREME COURT LANE | LEVEL 6 | SINGAPORE 178879 ABLI.ASIA | INFO@ABLI.ASIA

The Future of Privacy Forum (FPF) is a global non-profit organization that brings together academics, civil society, government officials, and industry to evaluate the societal, policy, and legal implications of data use, identify the risks, and develop appropriate protections. FPF has offices in Washington D.C., Brussels, Singapore, and Tel Aviv.

1350 EYE STREET NW | SUITE 350 | WASHINGTON, DC 20005 FPF.ORG | INFO@FPF.ORG