Asia-Pacific Privacy Legislation Tracker

Australia

Last updated 16 September 2025

Overview of Personal Data Protection Laws

What is the principal legislation, law or regulation governing personal data protection?	The principal data protection legislation in Australia is the Privacy Act 1988 (Cth) ('Privacy Act'). It includes 13 Australian Privacy Principles (APPs) that regulate the collection, use and disclosure of personal information.
Do the jurisdiction's data protection laws have extra-territorial scope?	Yes, the Privacy Act applies to the actions of agencies outside of Australia and to the actions of organisations and small business operators if they have an "Australian link". That is, if: (a) it has an organisational connection to Australia. For example, it is an Australian-established trust or a company incorporated in Australia; or (b) it conducts business in Australia or an external territory.

Key definitions under data privacy laws

What are the definitions of: (a) personal data, and (b) sensitive personal data under data protection laws?	**a. Provide examples to distinguish between "personal data" and "sensitive personal data."** The Privacy Act defines "personal information" as information or an opinion about an identified or reasonably identifiable individual. This is irrespective of the truth of that information or whether it is recorded in a material form or not. The Act defines "Sensitive information" as a type of personal information. It includes: (a) Information or opinion about an individual's:

- racial or ethnic origin
- political opinions or political association membership
- religious or philosophical beliefs
- membership of a professional or trade association or trade union
- sexual orientation or practices
- criminal record

(b) Health information;
(c) Genetic information (that is not health-related);
(d) Biometric information used for automated verification or identification and
(e) Biometric templates

What (if any) exceptions apply to the above definitions of personal data or sensitive personal data?	Private sector employee records are exempt from the Act, if they directly relate to an individual's current or former employment relationship.

Controller vs Processor

Do the jurisdiction's data protection laws include the concept of: (a) a "controller", and (b) a "processor"? How are they defined?	No, there is no recognised concepts of, or distinctions between, "data processors" or "data controllers". Rather, there are only "APP entities", that being entities regulated by the Privacy Act.
Do controllers have any legal obligations to control how processors manage the personal data that the controllers provide to them?	Whilst there is no distinction between "data processors" and "controllers" under the law, organisations are responsible for protecting personal data even when using third-party service providers. Any disclosure of personal information to a contractor or partner must still comply with the APPs, including APP principle 6 which limits the use or disclosure of personal information for the purpose for which it was collected. It also includes APP principle 7 which prohibits an organisation from using or disclosing personal information it holds for the purpose of direct marketing unless an exception applies.

Additionally, per APP principle 8, before transferring personal data abroad, an organisation must take reasonable steps to ensure the overseas recipient will handle the information in accordance with the APPs.

Legal basis for collection and processing

What are the legal bases permitting an organization to collect and process personal data?

Consent:

(a) What are the conditions or requirements for obtaining valid consent?

Even if an individual consents, an organization may not collect personal information unless it is reasonably necessary for one or more of their functions or activities.

However, an organization can use or disclose (as opposed to collect) personal information about an individual if they consent. An entity 'uses' information (that is within the entity's effective control) when it handles or undertakes an activity with the information. 'Disclosure' of information occurs when information is made accessible to others and the effective release of control the entity had over the information.

Consent needs to be voluntary, informed, current and specific, and the individual must have the capacity to understand and communicate their consent.

In order to have capacity to consent, the individual must:

- understand they are being asked to decide to give or not give consent;
- understand the consequences of giving or not giving consent;
- have based their decision on reason;
- be able to communicate their decision.

In general however, consent is not required to collect personal data and for using or disclosing personal information for a purpose for which it was collected. Rather, it is an exception that allows for using or disclosing personal information for a secondary purpose.

(b) Does the jurisdiction's data protection law recognize

different types of consent?

Consent can be implied or express, depending on the circumstances and sensitivity of the information.

(c) Can consent be withdrawn?

Yes, a person can withdraw consent at any time. Once withdrawn, an agency or organization is not able to rely on a person's past consent.

□ "Legitimate interests":

(a) What interests are considered legitimate interests?

(b) For an organization to rely on "legitimate interests", what are the relevant requirements or conditions?

□ "Contractual necessity":

(a) What purposes would fall under this legal basis?

(b) For an organization to rely on this legal basis, what are the relevant requirements or conditions?

□ Compliance with legal / regulatory requirement":

(a) What purposes would fall under this legal basis?

An agency may collect, use or disclose personal information if it is *"required or authorized by or under an Australian law, or a court/tribunal order".*

(b) For an organization to rely on this legal basis, what are the relevant requirements or conditions?

To rely on the "required by law or court/tribunal order" basis, they must show that they have a legal obligation with no discretion to act differently.

To rely on the "authorized by law or court/tribunal order" basis, they must show clear legal permission, even if not mandatory.

Australian law includes Acts, regulations, instruments and common law/equity but not contracts and a court/tribunal order includes an order or direction by a court, tribunal or judicial officer.

Other legal basis apart from the above:

(c) What are the other legal bases?

For personal information, an organization or agency must only collect this information where it is reasonably necessary for one or more of their functions or activities. In addition, agencies may collect personal information that is directly related to their functions or activities.

Personal information should be collected by lawful and fair means and collected directly from the individual concerned, unless it is unreasonable or impracticable to do so.

Additionally, at or before the time of collection (or as soon as practicable thereafter) the organization must notify the individual or key matters including:

- the purpose of the collection;
- the organization's identity and contact details;
- any third parties to whom the data might be disclosed; and
- the fact that the individual can access or correct their information.

Organizations can only use or disclose personal information for the primary purpose for which it was collected, or for a secondary purpose if an exception applies.

(d) What purposes would fall under each legal basis mentioned above in 5.a?

An organization's functions or activities include:

- the organization's existing functions or activities;
- planned functions or activities the organization has formally decided to undertake and developed implementation plans for; and
- supporting activities that enable the organization to perform its functions, such as human resources, corporate administration, property management, and public relations

The primary purpose of collection refers to the specific activity or function for which an entity collects personal information, and personal information may only be used or disclosed for this purpose unless an

exception applies.

In addition to the exceptions of consent and being required or authorized by Australian law or a court/tribunal order, exceptions include:

The individual would reasonably expect the entity to use or disclose their personal information for the secondary purpose, and the secondary purpose is related to the primary purpose of collection.

A permitted general situation applies in relation to the secondary use or disclosure. Permitted general situations include:

- lessening or preventing a serious threat to life, health or safety;
- taking appropriate action in relation to suspected unlawful activity of serious misconduct;
- locating a person reported as missing;
- establishing, exercising or defending a legal or equitable claim;
- conducting a confidential alternative dispute resolution process;
- necessary for a diplomatic or consular function or activity (applies only to agencies);
- necessary for certain defense force activities outside Australia (applies only to the Defense Force).
- The entity is an organization, and a permitted health situation applies in relation to the secondary use or disclosure. Permitted health situations include:
- conducting research; compiling or analyzing statistics; management, funding or monitoring of a health service necessary to prevent a serious threat to the life, health or safety of a genetic relative; and
- disclosure to a responsible person for the individual.
- The entity reasonably believes the secondary use or disclosure is reasonably necessary for one or more enforcement-related activities conducted by, or on behalf of, an enforcement body.
- The entity is an agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, in accordance with guidelines issued by the

Information Commissioner under APP 6.3.

(e) For an organization to rely on each legal basis mentioned above in 5.a, what are the relevant requirements or conditions?

An entity must be able to show that there is objective necessity, i.e. that a reasonable person who is properly informed would agree the collection is necessary. Factors relevant to determining whether it is reasonably necessary include:

- the main purpose for which the information is being collected;
- how the information will be used in carrying out the APP entity's function or activity — noting that collecting information solely because it might be useful in the future will usually not meet the "reasonably necessary" threshold;
- whether the entity could perform the function or activity without collecting the information, or by collecting less information.

If local law recognizes the concept of "sensitive" personal data, are there special rules to the legal bases mentioned in Q.1, or different legal bases than the above, for an organization to collect or process sensitive personal data?

a. What are the special rules / different legal bases?
Organizations must not collect sensitive information about an individual unless the individual has given consent **and** the collection is reasonably necessary for one of the entities functions or activities.

Exceptions to this requirement include where:

- the collection of sensitive information is required or authorized by law or a court/tribunal order;
- a permitted general situation exists;
- a permitted health situation exists;
- it is for an enforcement related activity;
- it is by a non-profit organization.

Additionally, any APP entity, including an organization, may collect sensitive information if the collection "is required or authorized by or under an Australian law or a court/tribunal order".

b. For an organization to rely on each legal basis mentioned above in (a), what are the relevant requirements or conditions?

In order to qualify for enforcement related activity, enforcement bodies must reasonably believe the collection is reasonably necessary for or directly related to their functions or activities. The Immigration Department must reasonably believe the collection is reasonably necessary for or directly related to its enforcement-related activities.

For non-profit organizations, the sensitive information must relate to the organization's specified activities; be connected to a member or someone in regular contact with the organization; and be objectively related to the activity being conducted.

Transparency / disclosure requirements

Are there any transparency or disclosure requirements under the jurisdiction's data protection laws, requiring disclosure of certain information to data subjects? If yes – What are the items of information that must be disclosed to data subjects?

Under APP 5, when an organisation collects personal information, it must take reasonable steps to notify the individual of specific matters. This includes:

- The identity of contact details of the organisation collecting the information.
- If the data is collected from a third party and not directly from the individual, they should be informed of that and how/why it was collected.
- If the collection is required or authorised by an Australian law or court order, this must be stated (including naming the law or order).
- The primary purposes for which the information is being collected.
- The main consequences (if any) for the individual if they don't provide the information
- They types of other entities or persons to whom the organisation usually discloses that kind of personal information.
- Reference to the organisation's privacy policy, specific noting that the policy contains information about how individuals may access and correct their information, and how to complain about a privacy breach.

- Whether the organisation is likely to disclose the personal information to overseas recipients, and if so, the countries in which those recipients are likely to be located (if practicable to specify).

Are organizations required to have a privacy policy? If yes, must the privacy policy cover the information as in the 'Overview of Personal Data Protection Laws' above, or is any additional information required to be covered?

The Privacy Act requires organisations to have a freely available, clear and up to date privacy policy addressing their overall data handling practices. At a minimum, the policy must cover:

- The kinds of personal information collected and held.
- How the entity collects and holds that personal information.
- The purposes for which the entity collects, uses, and discloses personal information.
- How individuals can access their personal information and seek correction if needed.
- How individuals can complain and how the organisation will handle that complaint.
- Whether the entity is likely to disclose personal information overseas and, if so, the countries in which recipients are likely to be located (if practicable).

Data of children or minors

Are there specific laws, regulations, rules or guidelines that govern the collection or processing of children's personal data?

Australia does not have a dedicated children's data protection statute and The Privacy Act applies to personal information of individuals at any age.

However, the Office of the Australian information Commission (OAIC) has issued guidance on handling children's personal information. Where consent is required (for example, for collecting sensitive information), organisations must assess an under-18 individual's capacity to consent on a case-by-case basis, taking into account the young person's maturity and ability to understand what is being proposed with their data. Where a child lacks the maturity to understand the implications, it is appropriate to seek consent from a parent or guardian on the child's behalf.

If it is not practical to assess capacity individually, as a general rule, the

OAIC suggests that an organisation may assume that individuals aged 15 and older have capacity to make their own privacy decisions, unless there is something to suggest otherwise.

What mandatory requirements do those laws, regulations, rules or guidelines provide for the collection or processing of children's personal data?

a. **If consent applies in respect of collecting or processing children's personal data, what constitutes valid consent?**

Handling children's personal data must comply with the same laws as for adults. Where consent is required, for that consent to be valid, the individual must have capacity to consent.

That is, the individual must:

- understand they are being asked to decide to give or not give consent;
- understand the consequences of giving or not giving consent;
- have based their decision on reason;
- be able to communicate their decision.

Children-specific considerations to determining whether consent is valid is discussed in Q.1 above.

Direct and e-marketing online tracking and cookies requirements

What constitutes direct marketing under the jurisdiction's data protection laws?

Whilst the Privacy Act does not define "direct marketing", the concept is described in the APP 7 Guidelines. In essence, direct marketing involves using or disclosing personal information to communicate directly with an individual to promote goods. An organization must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies (see q 2. below).

What are the requirements for the use of personal data for direct marketing or e-marketing?

- **Consent. What are the consent requirements specific to direct marketing or e-marketing?**

Direct-marketing

For sensitive information, an organisation may only use or disclose that information for direct marketing if the individual has consented to the use or disclosure for that purpose.

For non-sensitive, personal information:

- If the information was collected directly from the individual and they would reasonably expect it to be used for direct marketing, consent is not required; and
- If the personal information was collected from a third party, or the individual would not reasonably expect its use for direct marketing, the organisation must obtain consent, or it must be impracticable to obtain consent.

Commercial electronic messages

The sending of commercial electronic messages, primarily email, SMS and MMS marketing, is governed under The Spam Act 2003 (Cth). Where the Spam Act applies, the Privacy Act does not.

Under the Spam Act, commercial emails or texts must not be sent without the recipients prior consent. The body responsible for enforcing the Spam Act, the Australian Communications and Media Authority (ACMA) advises that express consent should be obtained on the basis of clear and accessible terms and conditions, provided to recipients at the time consent is sought—for example, by completing a form, ticking a box online, over the phone, or in person.

Disclosure. What are the requirements for disclosing information to data subjects which are specific to direct marketing or e-marketing?

Direct Marketing

Organisations are required to include a simple means for individuals to opt out of receiving direct marketing communications.

In cases where the personal information was collected from a third party, or the individual would not reasonably expect its use for direct marketing, each direct marketing communication is required to include a prominent statement that informs the individual of their opt-out right.

Commercial Electronic Messages

Each electronic message sent must clearly identify the sender and include a functional unsubscribe option that allows the recipient to opt out of all future electronic marketing communications

 Other requirements. What are the other requirements specific to direct marketing or e-marketing?

Direct Marketing

If requested, organisations must notify the individual of the source of their personal information, unless it is unreasonable or impracticable to do so.

Commercial Electronic Messages

Unsubscribe requests must be processed within 5 business days for electronic messages.

What specific laws, regulations or guidelines (if any) govern the use of cookies and similar online tracking tools?

Australia does not have a law dedicated solely to cookies or online tracking technologies. Instead, the use of cookies and similar online tracking tools is regulated indirectly through the Privacy Act if the data collected via those tools is "personal information".

The OAIC has issued guidance on tracking pixels, a common online tracking tool. It provides that the following types of information commonly collected by tracking pixels may be considered personal information for the purposes of the Privacy Act:

- Form inputs like name, address, date of birth, email address and phone number
- Transactional data like items viewed and cart additions
- Network information including IP addresses and geolocation data
- URL information
- Other activity data such as session duration, pages visited and content viewed.

What do those laws or guidelines require for the use of cookies or similar online tracking tools?

Organisations are required to comply with the same Privacy Act and the APP obligations they would with other just as they would with other means of collecting personal data. Organisations should regularly review their tracking technologies to ensure ongoing compliance.

Additionally, the OAIC provides that with regards to tracking pixels, organisations should ensure, as part of a data minimisation approach, that pixels are configured in such a way as to limit the collection of personal data to the minimum necessary amount.

When using tracking pixels to target individuals with online ads, organisations must comply with the direct marketing obligations discussed above, including providing individuals with a simple means to

opt-out.

Data sharing and engaging processors

Are there any requirements for sharing personal data or engaging third party data processors to process personal data?	Any disclosure of personal information to a contractor or partner must still comply with the APPs, including APP principle 6 which limits the use or disclosure of personal information for the purpose for which it was collected and APP principle 7 which prohibits an organization from using or disclosing personal information it holds for the purpose of direct marketing unless an exception applies. Additionally, per APP principle 8, before transferring personal data abroad, an organization must take reasonable steps to ensure the overseas recipient will handle the information in accordance with the APPs.

Data localization and cross-border transfer

Are there data localization or similar laws that require personal data to be retained in the local jurisdiction?	No, there is no overarching law that requires personal information to be stored or remain within Australian territory. Organizations subject to the Privacy Act are allowed to host or transfer data overseas, so long as they comply with the cross-border data protections rules (APP 8) and other APPs.
What are legal mechanisms for cross-border data transfers ?	Data subject consent a. Under APP 8.1, an APP entity must take reasonable steps to ensure that an overseas recipient does not breach the APPs before they disclose information. An individual however can consent to APP 8.1 not applying, if they are expressly informed that it will not apply. b. Once valid consent is obtained under these conditions, the APP is not required to take those reasonable steps, nor is the entity accountable for any acts or practices of the overseas recipient that would breach the APPs. Transfers to jurisdictions which are whitelisted or subject to an adequacy decision. a. An entity can disclose personal information to an overseas recipient without complying with APP 8.1 if it reasonably believes that: ◦ a law or binding scheme that protects the information in a

substantially similar way to the APPs applies to the recipient; and

- individuals have mechanisms available to them to enforce that protection.

b. If these conditions are met, the APP is not required to take reasonable steps to ensure the overseas recipient does not breach the APPs, nor is the entity accountable for any acts or practices of the overseas recipient that would breach the APPs.

- Standard data protection clauses (SCCs)
- Binding corporate rules (BCRs)
- Codes of conduct
- Certification mechanisms
- Ad hoc contractual clauses
- Approval from or registration or filing with local authorities

Data subject rights

What are the data subject rights provided under the jurisdictions' data protection law?

□ Right to be informed. What does this right require the organization to do?

At or before the time of collection (or as soon as practicable thereafter) the organization must notify the individual of key matters including:

- The purpose of the collection;
- The organisation's identity and contact details;
- Any third parties to whom the data might be disclosed; and
- The fact that the individual can access or correct their information.

Where the personal information is not collected directly from the individual, an organisation needs to take reasonable steps to ensure that the individual is informed of these matters.

□ Right of access. If applicable, what does this right require the organization to do?

APP 12 allows individuals to request access to personal information an organisation holds regarding them. The organisation must then provide the individual access to their data within a reasonable period and, if reasonable, in the manner requested.

□ Right to rectification. If applicable, what does this right require the organization to do?

APP 13 allows individuals to request the correction of any inaccurate, incomplete, out-of-date, irrelevant or misleading personal information. Organisations must, once they are notified or become aware of inaccuracies, take reasonable steps to correct the information.

□ Right to data portability. If applicable, what does this right require the organization to do?

If an individual requests to receive access to personal information in a reasonable manner (this could include a request for it to be in a portable format) , an organisation is required give access to information in the manner requested, if it is practical and reasonable to do so. If it is not able to, the organisation must, in a written notice, explain its reasons for not doing so.

Additionally, the Treasury Laws Amendment (Consumer Data Right) Act 2019 allows individuals access to certain categories of personal data held by designated organisations and transfer that data to:

- Accredited third parties, including consultants, other advisors and bookkeepers; and
- Certain unaccredited third parties, such as lawyers, financial advisors and mortgage brokers.

□ Right to object. What does this right require the organization to do?

Individuals are allowed to lodge a complaint with the organisation, and then if necessary, to the OAIC. Organisations must have a process for handling privacy complaints and are to describe this in their privacy policy.

 Rights related to automated decision making including profiling. If applicable, what does this right require the organization to do?

Data protection impact assessments

In what circumstances are data protection impact assessments required?	For government agencies, a Privacy Impact Assessment (PIA) is mandatory, under the Australian Government Agencies Privacy Code, for all "high privacy risk" projects. This includes maintenance and publication of a PIA registrar. For private organisations, PIA's are not legally required. However, OAIC guidance for APP 1 suggests that PIA's for new personal data initiatives are a reasonable step towards good privacy governance.

Data Protection Officer

Is there a requirement to appoint a DPO? If yes:	Yes.
In what circumstances is it required to appoint a DPO?	For private organisations, there is no requirement to appoint a DPO under Australian law. For federal agencies subject to the Privacy Act, there is a requirement to appoint a "Privacy Officer" and a "Privacy Champion".
Does the DPO have to possess certain qualifications or meet specific requirements? If so, what are these qualifications or requirements?	There are no stated requirements for a Privacy Officer, however a Privacy Champion is to be a senior official within the agency.
What are the responsibilities of a DPO?	A Privacy Officer is responsible for ensuring day-to-day operational privacy activities are undertaken. They will be the first point of contact for privacy matters within the agency. The role of a Privacy Champion is to be responsible for leadership activities and engagement that necessitate broader strategic oversight.

Registration notification or filing requirements

Are there obligations to register with or notify the data protection authority in order to collect or process personal data generally?	There is no general legal requirement to register data processing activities nor to notify the OAIC before collecting or processing personal data.

Security requirements and breach notification

What obligations does the jurisdiction's data protection law impose, with respect to maintaining security controls to protect personal data from unauthorized access?	APP 11 requires organisations to take reasonable steps to protect personal information from interference, loss, unauthorised access, modification, disclosure or other misuse. Organisations must implement measures that are appropriate after taking into account their size, the sensitivity of information and potential adverse consequences of a breach. They also must de-identify or destroy personal information that is no longer required, unless the retention of that information is part of a Commonwealth record or is required by law.
How is a "data breach" or "data incident" defined?	The Privacy Act does not define the term "data breach" and relies on their ordinary meaning. Generally, "data breach" refers to any access or disclosure of personal information that is unauthorised, or the loss of personal information by an entity.
Are there mandatory obligations on the steps an organization is required to take in the event of a data breach / incident?	Yes. The first obligation is to contain the breach where possible and take remedial action. If an organisation suspects that a data breach is one that is likely to result in serious harm to individuals (an "eligible data breach"), it is required to promptly conduct a reasonable assessment whether this has occurred. In the event that this assessment finds that an eligible data breach has occurred, the entity needs to notify the OAIC by preparing and submitting a statement explaining the breach. It is also required to notify the impacted individuals.

Are there mandatory obligations to notify a regulator or data subjects about a personal data security breach?

a. When is a notification obligation triggered:

- Quantitative threshold (e.g. volume of data or number of data subjects involved)
- Qualitative threshold (e.g. sensitivity of data or risk posed to data subjects)

Notification is required if a breach is likely to result in "serious harm" to any individuals whose information is involved.

'Serious harm' may include, for example:

1. Identity theft
2. Financial loss through fraud
3. Likely risk of physical harm, e.g. by an abusive ex-partner
4. Serious psychological harm
5. Serious reputational harm

b. What is the timing requirements for making a notification?

An organisation or agency is expected to, within 30 days, assess whether a data breach is likely to result in serious harm and therefore requires notification. The notification must be issued as soon as practicable.

c. What content must the notification contain?

A notification is to include:

- The relevant organisation or agency's name and contact details
- A description of the breach, including what kinds of personal information were involved
- Recommended next-steps

d. Are there any other requirements for making notifications?

A notification may take the form of an email, text message or phone call.

If individual notification is not practicable (taking into account time, effort and cost), the entity must publish a copy of the statement prepared for the OAIC on its website as well as taking reasonable steps to bring the content of the statement to the attention of impacted individuals.

If multiple organisations are involved in a breach, generally, only one notification is required.

DP authority and enforcement focus penalties under DP laws

Who is the main data privacy authority or regulator in your jurisdiction?

Office of the Australian Information Commissioner (OAIC).

What are the penalties for non-compliance with local data protection laws?

a. Do data subjects have any private remedies?

For serious interferences with the privacy of individuals, the maximum penalty for companies is whichever is higher of:

- A $50 million; or
- Three times the value of any obtained benefit; or
- 30% of a company's adjusted domestic turnover in the relevant period of up to 12 months.

For individuals the maximum penalty for serious interferences is up to A$ 2.5 million.

For less-serious offences, the OAIC is also able to issue infringement notices resulting in the payment of civil penalties.

Data subjects don't have a direct right to sue for a breach of the Privacy Principles, only the right to complain.

Has the data privacy regulator issued any notable enforcement guidance or judgments in the last 12-24 months?

In December 2024, the OAIC announced a $50 million settlement with a social media company after it commenced proceedings in 2020 alleging that it had disclosed, without consent, over 300,000 Australian users' data to another entity.

In June 2024, the OAIC filed civil penalty proceedings against an entity for allegedly failing, in relation to a 2022 medical records breach affecting approximately 9.7 million people and exposing highly sensitive health data, to take reasonable security steps.

In mid-2023, the Administrative Appeal Tribunal (AAT), affirmed the OAIC's approach to extraterritorial application to the Privacy Act.

The OAIC, in October 2024, published guidance on privacy and Artificial intelligence (AI). Specifically:

- Guidance on privacy and the use of commercially available AI products; and
- Guidance on privacy and developing training generative AI models.

The OAIC in the same month also released updated privacy guidance for not-for-profits, providing expanded advice on steps that not-for-profits can put in place to ensure compliance and improve security of information.

Associated Contacts

Charmian Aw

Email Me

Ciara O'Leary

Email Me

Mainland China

Last updated 17 September 2025

Overview of Personal Data Protection Laws

What is the principal legislation, law or regulation governing personal data protection?	Personal Information Protection Law ("**PIPL**"), which came into full force on November 1, 2021.
Do the jurisdiction's data protection laws	

have extra-territorial scope?	Yes. The processing carried out by Mainland China-located personal information handler (i.e., organizations and individuals that independently determine the purposes and methods of personal information processing) is naturally subject to the PIPL. Where any offshore personal information handler processes the personal information of China-based data subjects outside of China in order to provide products or services to individuals in China, or analyze the activities of individuals in China, or as otherwise prescribed by law, the PIPL shall apply to this offshore entity.

Key definitions under data privacy laws

What are the definitions of: (a) personal data, and (b) sensitive personal data under data protection laws?	**a. Provide examples to distinguish between "personal data" and "sensitive personal data."** 1. Personal information is defined as various types of information, recorded in electronic or other forms, that relate to an identified or identifiable natural person. It does not include information that has undergone anonymization processing. 2. Sensitive personal information means personal information that if leaked or used unlawfully, may easily cause harm to the dignity of data subjects or serious harm to personal security or the security of property, including biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking and the personal information of minors under the age of 14. It is important to note that the PIPL's definition of sensitive personal information is non-exhaustive.
What (if any) exceptions apply to the above definitions of personal data or sensitive personal data?	No

Controller vs Processor

Do the jurisdiction's data protection laws include the concept of: (a) a "controller", and (b) a "processor"? How are they	Yes. The personal information handler (equivalent to the "controller") is defined as the organizations and individuals that independently determine the purposes and methods of personal information processing. The entrusted personal information processor (equivalent to "processor") generally refers to an organization or individual that

defined?	accepts entrustment from a "personal information handler" and processes personal information on its behalf in accordance with the provisions of the entrustment agreement.
Do controllers have any legal obligations to control how processors manage the personal data that the controllers provide to them?	Yes. A personal information handler is responsible for ensuring that its entrusted data processor's processing activities complying with the same obligations under the PIPL, as if the personal information were processed by the personal information handler itself.

Legal basis for collection and processing

What are the legal bases permitting an organization to collect and process personal data?	**□ Consent:** (a) What are the conditions or requirements for obtaining valid consent? Firstly, the individual must have been informed of the details (see Row 5 for more details) for the processing of his/her personal information on or before collecting that information. Secondly, the consent must not be as a condition of providing a product or service, beyond what is reasonable to provide that product or service. Thirdly, consent must not have been obtained using any deceptive or misleading practices, i.e., the consent shall be given freely and specific. (b) Does the jurisdiction's data protection law recognize different types of consent? No. That said, there is a national standard that, while non-mandatory, is frequently cited and specifies that consent may be deemed "obtained" under certain circumstances, for instance, if an individual voluntarily provided his/her personal information to the organization; an individual continues to choose to enter or remain in an image capture area with knowledge of the area's existence. (c) Can consent be withdrawn? Yes. **□ "Contractual necessity":** (a) What purposes would fall under this legal basis? Any processing (collection, use or disclosure) of an individual's personal information, for the conclusion and/or performance of a

contract" in which the data subject is an interested party", subject to the conditions in the sub-paragraph (b) which immediately follows.

(b) For an organization to rely on this legal basis, what are the relevant requirements or conditions? To qualify for the contractual necessity exemption, the personal information processed on the basis of this legal ground must be essential to either concluding the contract in question or performing the obligations thereunder. Notably, data collected solely for service improvement purposes (e.g., analytics and cookies) cannot generally rely on this exemption.

- **"Compliance with legal / regulatory requirement":**

(a) What purposes would fall under this legal basis? Any processing (including collection, use or disclosure) of personal information to fulfil statutory obligations.

(b) For an organization to rely on this legal basis, what are the relevant requirements or conditions? The processing must be necessary to comply with a legal or regulatory requirement imposed by law.

Other legal basis apart from the above:

(a) What are the other legal bases? (i) where it is necessary to conduct human resources management in accordance with labor rules and collective employment contracts; (ii) where it is necessary to respond to sudden public health incidents or to protect individuals' lives and health or the security of their property in emergency situations; (iii) where the processing is within a reasonable scope for news reporting, public opinion supervision and other such activities in the public interest; (iv) where the processing is within a reasonable scope of personal information already disclosed by the data subjects or lawfully disclosed.

(b) What purposes would fall under each legal basis mentioned above in (a)? Please see above.

(c) For an organization to rely on each legal basis mentioned above in (a), what are the relevant requirements or conditions? The personal information to be processed must be strictly necessary for the aforementioned purposes, and when applicable, such processing shall be conducted within a reasonable scope specific to the intended processing activity. Currently, the PIPL does not

provide further clarification on the definitions of "necessity" and "reasonableness."

If local law recognizes the concept of "sensitive" personal data, are there special rules to the legal bases mentioned in Q.1, or different legal bases than the above, for an organization to collect or process sensitive personal data?	(a) What are the special rules / different legal bases? Not applicable. (b) For an organization to rely on each legal basis mentioned above in (a), what are the relevant requirements or conditions? For the processing of sensitive personal information based on consent, personal information handler shall obtain separate consent from the data subject, i.e., an individual's specific and explicit consent given solely for the purpose of conducting a particular processing of their personal information. As a market compliance practice, it is advised to provide multiple tick boxes for requesting separate consent for each applicable processing.

Transparency / disclosure requirements

Are there any transparency or disclosure requirements under the jurisdiction's data protection laws, requiring disclosure of certain information to data subjects? If yes – What are the items of information that must be disclosed to data subjects?	Generally, unless otherwise exempted, the personal information handler shall notify the following items to the data subjects: ◦ the name and contact information of the personal information handler; ◦ the purposes and means of processing, and the categories and storage periods of the personal information to be processed; ◦ the methods and procedures for the data subject to exercise his rights as provided in the PIPL; and ◦ ·other matters that the data subject should be notified of as provided by laws and administrative regulations. Specifically – ◦ for processing of sensitive personal information, the data subjects must be notified of the necessity of processing sensitive personal information and the impact on their rights and interests; ◦ for transfers of personal information from one personal information handler to another, it is required to notify data

subjects of the name, contact method, purpose and methods of information processing and the categories of personal information being shared with the transferee; and

- for transfers of personal information to offshore data recipient, it is required to notify data subjects of the name of the offshore data recipient, contact information, purpose and method of processing, type of personal information and the method and procedure for the individual to exercise the rights against the overseas recipient.

Are organizations required to have a privacy policy? If yes, must the privacy policy cover the information as in the 'Overview of Personal Data Protection Laws' above, or is any additional information required to be covered?	No, PIPL does not provide requirements on the form to disclose the processing rules. Specifically, in the case of data processing conducted via the Internet, if a personal information handler chooses to fulfill its transparency obligation by formulating personal information processing rules, it shall disclose the purpose, method, and type of personal information to be collected and transferred, as well as the data recipient's information (where applicable), in the form of a checklist or other equivalent means.

Data of children or minors

Are there specific laws, regulations, rules or guidelines that govern the collection or processing of children's personal data?	Yes – ◦ Law of the People's Republic of China on the Protection of Minors (amended in 2024); ◦ Provisions on the Protection of Minors' Personal Information in Cyberspace (effective on October 1, 2019); ◦ Measures for the Protection of Personal Information of Children in Difficult Circumstances (effective on November 18, 2024); ◦ Recommended Industrial Standards, like the Technical Requirements for the Protection of Minors' Personal Information in Mobile Internet Applications and the Technical Requirements for Notification and Consent in the Processing of Children's Personal Information by Mobile Internet Applications.

What mandatory requirements do those laws, regulations, rules or guidelines provide for the collection or processing of children's personal data?

a. **If consent applies in respect of collecting or processing children's personal data, what constitutes valid consent?**

If consent applies in respect of collecting or processing children's personal information, what constitutes valid consent?

As a rule of thumb, for any individual that is under the age of 14, his/her parental or legal guardian's consent would be required (if no other legal basis available) before an organization can process his/her personal information. Minors aged 14-18 are "persons with limited capacity for civil conduct" under the Chinese Civil Law, while minors aged 16-18 with independent income are deemed full civil capacity thereunder. For minors aged 14-18: while they may independently consent to personal information processing comprehensible to them, it is still advisable to obtain consent to sensitive information processing from their guardians as a conservative approach. Notably, for registering as a live streaming publisher, even minors aged 16-18 must obtain guardian consent to comply with industry-specific regulations

Direct and e-marketing online tracking and cookies requirements

What constitutes direct marketing under the jurisdiction's data protection laws?

Direct marketing is not specifically defined but would refer to any marketing that is sent to a person using his/her contact details such as a telephone number, email address, or postal address.

What are the requirements for the use of personal data for direct marketing or e-marketing?

- **Consent. What are the consent requirements specific to direct marketing or e-marketing?**

Generally, consent is required for direct marketing including e-marketing to individuals.

- **Disclosure. What are the requirements for disclosing information to data subjects which are specific to direct marketing or e-marketing?**

As nothing additional is specifically prescribed, the usual notification obligations would apply, so data subjects need to be informed of the purposes of processing their personal information, such as the types of marketing that they will be receiving unless they have opted out.

- **Other requirements. What are the other requirements**

	specific to direct marketing or e-marketing?
	N/A
What specific laws, regulations or guidelines (if any) govern the use of cookies and similar online tracking tools?	Not Applicable
What do those laws or guidelines require for the use of cookies or similar online tracking tools?	Not Applicable

Data sharing and engaging processors

Are there any requirements for sharing personal data or engaging third party data processors to process personal data?	**Transfer to another Personal Information Handler** Transfers of personal information from one personal information handler to another require a personal information protection impact assessment and "separate consent" unless the personal information handler can rely on other lawful basis (such as necessary for the performance of contract) to justify the data transfer. Personal information handlers are required to notify data subjects of the name, contact method, purpose and methods of data processing and the categories of personal data being shared with the transferee. It is mandatory for the network personal information handler (personal information handler that process personal information via Internet) to implement a data transfer agreement with the data recipient (acting as another network personal information handler) to specify the processing purpose, method and scope as well as the security protection obligations of the data recipient, and supervise the data recipient's performance of such obligations. Records of providing personal data to other network personal information handlers shall be kept for at least three (3) years. **Transfer to Entrusted Personal Information Processor** The PIPL imposes general obligations in respect of personal information handlers' "entrustment" of personal information with entrusted processors. Personal information handlers are required to enter into

agreements with the entrusted personal information processors specifying:

- the purpose of the entrustment;
- the duration of the entrustment;
- the categories of personal information being processed;
- the method of processing;
- the protection measures applied to the data processing; and
- the parties' respective rights and obligations in processing the personal information.

Personal information handlers are required to supervise data processing by the entrusted personal information processors. Records of entrustment of processing personal information shall be kept for at least three (3) years.

The entrusted personal information processors are required to comply with the terms and conditions of entrustment agreements and delete or return personal information once the entrustment is not effective, invalid, terminated, or revoked. The entrusted personal information processors are not permitted to process personal information for purposes or using methods beyond the authorization under the entrustment and may not delegate their processing of the personal information without the consent of the personal information handlers.

Data localization and cross-border transfer

Are there data localization or similar laws that require personal data to be retained in the local jurisdiction?

Yes. Under Article 40 of the PIPL, organizations which: (i) are an operator of critical information infrastructure ("**CIIO**"); or (ii) handle personal information reaching prescribed thresholds (these are currently unspecified but parties could use the thresholds that would trigger the security assessment by the Cyberspace Administration of China ("**CAC**") as a reference), are required to localize personal information domestically collected and generated within Mainland China, unless it is passed by the CAC security assessment. CIIOs are companies engaged in important industries, including public communications, energy, transport, finance, national defense, etc., and designated by the CAC and industry supervising authorities as such. Note also that, depending on

the sector (for example, the financial sector), there may be other data localization requirements under other applicable laws. This is outside the scope of this advice.

What are legal mechanisms for cross-border data transfers ?

 Data subject consent.

 Transfers to jurisdictions which are whitelisted or subject to an adequacy decision.

 Standard data protection clauses (SCCs).

 Binding corporate rules (BCRs).

 Codes of conduct.

 Certification mechanisms.

 Ad hoc contractual clauses.

 Approval from or registration or filing with local authorities.

(a) For each of the applicable mechanisms, what are the requirements for the organization seeking to transfer personal information to rely on such mechanism?

To carry out cross-border transfers of personal information and important data, the transfer must be necessary for business operations, and the following requirements must be fulfilled.

(i) Regulatory Formalities

Under the PIPL and its implementation rules, the personal information handler (as the data exporter) shall satisfy at least one of the regulatory formalities (i.e. passing the Security Assessment by the CAC, concluding standard contractual clauses or obtaining third-party certification), subject to certain thresholds and exemptions as set out below, unless otherwise provided in the international treaties or agreements concluded or acceded to by China. Below, we set out the detailed requirements:

The CAC Security Assessment

If any of the following circumstances are triggered, the data exporter shall pass the security assessment by the CAC:

- the transferred data includes important data (e.g., data that raises national security/strategic sensitivities);
- the data exporter is identified as the operator of critical

information infrastructure ("CIIO");

- the data exporter other than the CIIO has cumulatively made international transfers of personal information (excluding sensitive personal information) of more than one million individuals or sensitive personal information of more than 10,000 individuals, from 1 January of the current year.

Standard Contractual Clauses

If none of the above-mentioned circumstances are triggered, the data exporter could conclude the standard contractual clauses published by the CAC ("**SCCs**") with the data recipient and conduct a record-filing with the CAC within 10 business days after the SCCs become effective.

Specifically, the SCCs approach will apply when the data exporter, other than the CIIO, has cumulatively made international transfers of personal information (excluding sensitive personal information) of more than 100,000 individuals but less than one million individuals, or sensitive personal information of less than 10,000 individuals, from 1 January of the current year.

Third-Party Certification

Obtaining a certification by a qualified third-party professional institution is an alternative approach for the SCCs, where the above SCCs thresholds are met.

(ii) Separate consent

The data handler should obtain separate consent from data subjects to export personal information outside of China, if the processing is based on the consent. In addition, the personal information handler should inform the data subject of the name of the overseas recipient, contact information, purpose and method of processing, type of personal information and the method and procedure for the individual to exercise the rights against the overseas recipient.

(iii) Other requirements

The PIPL also requires the personal information handler to conduct a PIA for the exportation and take necessary measures (unspecified) to ensure the processing activities of the offshore recipients will meet the PIPL standards.

(b) What if any derogations are permitted by law? Exemptions from Regulatory Formalities are as follows. Note that the exemptions only apply to the need to perform the Regulatory Formalities, and do not exempt the personal information handler from separate consent and other requirements stated above.

No personal information or important data. Data generated during activities such as international trade, academic cooperation, cross-border transportation, cross-border manufacturing, and marketing, which do not contain personal information or important data.

Personal information collected and generated overseas and subsequently transferred to China for processing, provided that no domestic personal information or important data is introduced during the processing (an exemption that is most likely meant to address situations in which China-based shared services operations and outsourcing arrangements process data originating from outside Mainland China).

Exemption for "contractual necessity" – where it is really necessary to provide personal information overseas for the conclusion or performance of a contract to which the data subject is a contracting party, including cross-border shopping, cross-border payment, cross-border account opening, and examination services.

Exemption for emergency – where it is really necessary to provide personal information abroad in an emergency to protect the life, health and property safety of a natural person.

Exemptions for employment relationship – where it is really necessary to provide employees' personal information abroad for the purpose of conducting cross-border human resources management in accordance with the employment rules and regulations formulated in accordance with the law and collective contracts concluded in accordance with the law.

Exemptions for limited transfer – personal information handlers other than CIIO who have cumulatively provided personal information (excluding sensitive personal information) of less than 100,000 people to foreign countries since January 1 of the current year.

Exemption for statutory duties or obligations – where it is truly necessary for the network personal information handler (personal information handler that process personal information via Internet) to provide personal information overseas for the purpose of performing statutory duties or obligations. However, the applicable scope of this

exemption remains uncertain and should be further confirmed with the CAC. We expect this exemption should be limited to statutory duties and obligations prescribed under PRC law and as a result, its practical application would be restricted under the current regulatory regime.

Exemption for Free Trade Zone ("FTZ") – FTZ is entitled to formulate their own "negative data lists" stipulating the types of data that are subject to Regulatory Formalities. These lists must be prepared in accordance with the national data classification protection framework and may only be implemented with the approval of the provincial CAC. Data exporters based in FTZs would be exempt from performing Regulatory Formalities provided that the data does not appear on the negative list.

Data subject rights

What are the data subject rights provided under the jurisdictions' data protection law?

 Right to be informed. What does this right require the organization to do? The personal information handler shall provide notification to individuals about the ways in which their personal information is processed, including making available the business contact details of its data protection officer.

 Right of access and to obtain a copy. What does this right require the organization to do? The personal information handler shall provide a requesting individual with personal information about him/her that is in its possession or under its control, and information about the ways in which the personal information has been used or disclosed by the organization.

 Right to rectification.What does this right require the organization to do? The personal information handler shall correct an error or omission in the personal information about the requesting individual that is in the possession or under the control of the organization.

 Right to erasure. What does this right require the organization to do? Individuals may exercise their right to request deletion in the following situations:

- where the purpose of processing has been achieved, cannot be achieved, or is no longer necessary to achieve;
- where personal information handler ceases to provide products or services, or the retention periods have expired;

- where data subjects withdraw consent and there is no other lawful basis for processing;
- where data subjects consider that a personal information handler processes their personal information in violation of laws, administrative regulations or the agreement; or
- ·other circumstances stipulated by PRC laws and administrative regulations.

 Right to restrict processing. What does this right require the organization to do? The personal information handler shall suspend certain personal information processing activities in terms of the personal information of the requesting individual.

 Right to data portability. What does this right require the organization to do? The personal information handler shall transfer the personal information of the requesting individuals to other personal information handlers, which meets the following conditions:

- where the true identity of the person making the request can be verified;
- where the personal information requested for transfer is the personal information that the individual has agreed to provide or has been collected on the basis of a contract;
- where the transfer of personal information is technically feasible; and
- where the transfer of personal information does not damage the legitimate rights and interests of others.

If the number of requests for transfer of personal information significantly exceeds a reasonable range, the network personal information handler may charge necessary fees based on the costs of transferring personal information.

Additionally, where the personal information handler refuses an individual's request to exercise his/her rights, the individual may file a lawsuit with a people's court. In the event of the death of an individual, a close relative of such an individual may exercise the right to access, make copies of, or have corrected or deleted, the relevant personal data of such an individual.

Data protection impact assessments

In what circumstances are data protection impact assessments required?	Under the PIPL, personal information handlers shall perform a personal information protection impact assessment, and keep a record of the course of the processing, before conducting the following activities: ◦ processing sensitive personal information; ◦ using personal information to conduct automated decision-making; ◦ entrusting personal information processing to another party, providing personal information for another party, or publicizing personal data; ◦ providing personal information to any party outside Mainland China; or conducting other personal information processing activities which may have significant impacts on individuals.

Data Protection Officer

Is there a requirement to appoint a DPO? If yes:	Yes.
In what circumstances is it required to appoint a DPO?	Personal information handlers that handle personal information of one million or more individuals must file a report on their DPO with the municipal-level CAC at their location./p>
Does the DPO have to possess certain qualifications or meet specific requirements? If so, what are these qualifications or requirements?	DPO shall take a specific position at the personal information handler, possess relevant work experience and professional knowledge in the field of personal information protection and be familiar with laws, administrative regulations, and other relevant provisions concerning personal information protection.
What are the responsibilities of	

a DPO?	DPO shall be granted adequate authority to effectively coordinate relevant departments and personnel within the personal information handler; has the right to put forward relevant opinions and suggestions before the decision-making process of major matters related to personal information processing; and has the right to directly stop non-compliant personal information processing within the personal information handler, and take necessary corrective measures

Registration notification or filing requirements

Are there obligations to register with or notify the data protection authority in order to collect or process personal data generally?	Not Applicable

Security requirements and breach notification

What obligations does the jurisdiction's data protection law impose, with respect to maintaining security controls to protect personal data from unauthorized access?	The personal information handler shall make reasonable security arrangements to prevent the unauthorized access, use, disclosure, modification and other similar risks to the personal information in its possession or control.
How is a "data breach" or "data incident" defined?	Not specifically defined under PIPL. It generally refers to the leak, distortion or loss of personal data that occurs or may have occurred.
Are there mandatory obligations on the steps an organization is required to take in the event of a	There are mandatory reporting requirements in cases which trigger such notifications – see our response to sub-question 14.4 below.

data breach / incident?	
Are there mandatory obligations to notify a regulator or data subjects about a personal data security breach?	a. When is a notification obligation triggered: □ Quantitative threshold (e.g. volume of data or number of data subjects involved). □ Qualitative threshold (e.g. sensitivity of data or risk posed to data subjects). PIPL requires personal information handlers to immediately take remedial actions and make notification to local CAC and data subjects (unless the personal information handler has adopted measures that effectively avoid harm, in which case individual notifications are not required, unless the authorities direct same). b. What is the timing requirements for making a notification? Without undue delay. c. What content must the notification contain? Notifications must include: (i) the categories of personal information impacted, the cause of the incident and the actual or potential harm caused by the incident; (ii) the remedial measures taken by the data subjects and measures that can be taken by data subjects to mitigate harm; and (iii) contact details for the personal information handler. d. Are there any other requirements for making notifications? Additionally, there are also other China laws and regulations provide the principles for reporting obligations of personal information handler in case of a data incident. There are multiple authorities involved, e.g., CAC, PSB (Public Security Bureau), and MIIT (Ministry of Industry and Information Technology). It is noted that those legal requirements are vague and lack detailed implementation measures, such as when companies must report, what is the threshold and what are the reporting procedures.

DP authority and enforcement focus penalties under DP laws

Who is the main data privacy authority or regulator in your jurisdiction?	CAC and its local counterparts.
What are the penalties for non-compliance with local data protection laws?	Where a personal information handler violates the provisions of PIPL in processing personal information, or fails to fulfill the personal information protection obligations prescribed by PIPL in processing personal information, CAC shall order rectification, issue a warning, and

confiscate illegal gains; for applications that illegally process personal information, CAC shall order the suspension or termination of service provision. If the personal information handler refuses to make rectification, a fine of not more than one million RMB shall be imposed in addition; and the persons in charge with direct responsibility and other persons directly liable shall be fined not less than 10,000 RMB but not more than 100,000 RMB.

If the illegal act specified in the preceding paragraph is serious, CAC at or above the provincial level shall order rectification, confiscate illegal gains, and impose a fine of not more than 50 million RMB or not more than five percent of the previous year's turnover; they may also order the suspension of relevant business operations or business rectification, and notify the relevant competent authorities to revoke the relevant business permits or business licenses. The persons in charge with direct responsibility and other persons directly liable shall be fined not less than 100,000 RMB but not more than one million RMB, and may be prohibited from serving as directors, supervisors, senior managers, or personal information protection officers of relevant enterprises for a certain period.

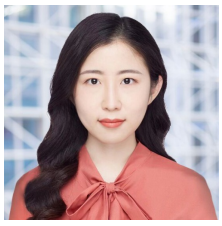
a. Do data subjects have any private remedies? Yes. Aggrieved individuals can bring a private action before the PRC courts.

Has the data privacy regulator issued any notable enforcement guidance or judgments in the last 12-24 months?	No

Associated Contacts

Sherry Gong

Email Me



Flora Feng

Email Me


Jessie Xie

Email Me


Ying Tang

Email Me

Hong Kong SAR

Last updated 17 September 2025

Overview of Personal Data Protection Laws

What is the principal legislation, law or regulation governing personal data protection?	The Personal Data (Privacy) Ordinance (Cap. 486 of the laws in Hong Kong) ("**PDPO**")
Do the jurisdiction's data protection laws have extra-territorial scope?	The PDPO does not, in general, have extra-territorial effect, except in relation to cessation notices issued to non-Hong Kong service providers regarding electronic doxing messages.

Key definitions under data privacy laws

What are the definitions of: (a) personal data, and (b) sensitive personal data under data protection laws?	**a. Provide examples to distinguish between "personal data" and "sensitive personal data."** Personal data is defined under the PDPO to mean any data (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable. There is no separate category or concept of sensitive data under the PDPO.

What (if any) exceptions apply to the above definitions of personal data or sensitive personal data?	None

Controller vs Processor

Do the jurisdiction's data protection laws include the concept of: (a) a "controller", and (b) a "processor"? How are they defined?	A data user, which is equivalent to the concept of controller in the GDPR context, is defined under the PDPO to mean a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of personal data. A data processor is defined under the PDPO to mean a person who processes personal data on behalf of another person, and does not process the data for any of the person's own purposes.
Do controllers have any legal obligations to control how processors manage the personal data that the controllers provide to them?	Yes, a data user must adopt contractual or other means: (i) to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data; and (ii) to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing

Legal basis for collection and processing

What are the legal bases permitting an organization to collect and process personal data?	**Consent:** (a) What are the conditions or requirements for obtaining valid consent? If a data user wishes to use personal data for a purpose which has not been notified to the data subject at the time of collection of the relevant personal data and is not directly related to the notified purposes (a "**New Purpose**"), Data Protection Principle ("**DPP**") 3 of the PDPO requires that the data user obtain the data subject's prescribed consent to this processing, which is the express voluntary consent which has not been withdrawn by written notice ("**Prescribed Consent**").

Consent is also required for using or transferring personal data for direct marketing purposes – see the responses to question 7 below.]

(b) Does the jurisdiction's data protection law recognise different types of consent?

Other than Prescribed Consent, the PDPO recognises consent specifically in a direct marketing context – see the responses to question 7 below.]

(c) Can consent be withdrawn?

Yes.

□ Other legal bases apart from the above:

(a) What are the other legal bases?

The PDPO is primarily a notification-based regime, in the sense that data users are allowed to collect and process personal data if they satisfy certain notification requirements under DPP 1(3) (see responses to question 5 below).

(b) What purposes would fall under each legal basis mentioned above in 5.a?

A data user should only use and process personal data for the notified purposes.

(c) For an organisation to rely on each legal basis mentioned above in 5.a, what are the relevant requirements or conditions?

In general, under DPPs 1(1) and (2) of the PDPO, personal data shall only be collected for a lawful purpose and only if necessary and not excessive for that purpose, by means which are (a) lawful; and (b) fair in the circumstances of the case.

If local law recognizes the concept of "sensitive" personal data, are there special rules to the legal bases mentioned in Q.1, or different legal bases than the above, for an organization to	Not Applicable

collect or process sensitive personal data?	

Transparency / disclosure requirements

Are there any transparency or disclosure requirements under the jurisdiction's data protection laws, requiring disclosure of certain information to data subjects? If yes – What are the items of information that must be disclosed to data subjects?	Under DPP 1(3), data users must take all practicable steps to notify data subjects of certain information on or before personal data collection, e.g., whether it is mandatory or voluntary for the data subject to provide the personal data, the purpose for which personal data is to be used, the classes of recipients to whom the personal data may be transferred, the data subject rights to request for access and correction of personal data, and details of the individual data subjects should contact to exercise data subject rights, etc. Additional notification requirements apply to the use or transfer of personal data for direct marketing – see the responses to question 7 below.
Are organizations required to have a privacy policy? If yes, must the privacy policy cover the information as in the 'Overview of Personal Data Protection Laws' above, or is any additional information required to be covered?	Yes. Under DPP 5, data users must take all practicable steps to make available information, including the data user's policies and practices in relation to personal data, the kind of personal data held by the data user and the main purposes such personal data is to be used.

Data of children or minors

Are there specific laws, regulations, rules or guidelines that govern the collection or processing of children's personal data?	The PDPO contains the concept of a relevant person, which in relation to a minor, refers to a person who has parental responsibility for the minor ("**Relevant Person**"). A Relevant Person is able to perform certain acts under the PDPO on behalf of a minor who is the data subject, including exercising data subject rights, making a complaint to the Hong Kong Privacy Commission for Personal Data ("**PCPD**"), or giving Prescribed Consent if the minor is incapable of understanding the New Purpose

	and deciding whether to give the consent, and the Relevant Person has reasonable grounds to believe that the use of personal data for the New Purpose is clearly in the minor's interests.
What mandatory requirements do those laws, regulations, rules or guidelines provide for the collection or processing of children's personal data?	Not Applicable

Direct and e-marketing online tracking and cookies requirements

What constitutes direct marketing under the jurisdiction's data protection laws?	Direct marketing under the PDPO refers to (a) the offering, or advertising of the availability, of goods, facilities or services; or (b) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes, by "direct marketing means", i.e. by sending information or goods addressed to specific persons by name, or making telephone calls to specific persons
What are the requirements for the use of personal data for direct marketing or e-marketing?	◦ **Consent. What are the consent requirements specific to direct marketing or e-marketing?** Consent in relation to direct marketing is defined under the PDPO to include an "indication of no objection" – the data subjects must take positive action to indicate that they do not object to the use of their personal data to direct marketing purposes ("**DM Consent**"). While oral consent is permitted in relation to the use of personal data for the data user's own direct marketing, written consent is required where personal data will be provided to third parties (including related / affiliated entities) for their use in direct marketing. ◦ **Disclosure. What are the requirements for disclosing information to data subjects which are specific to direct marketing or e-marketing?** Before using personal data for direct marketing purposes, data users must inform data subjects of certain information, e.g. the data user intends to use (or provide) personal data for direct marketing, and may

	not do so without the data subject's consent; the types of personal data to be used for direct marketing and the classes of marketing subjects concerned; the classes of recipient to whom personal data is provided for direct marketing, and whether such provision is for gain, etc.
What specific laws, regulations or guidelines (if any) govern the use of cookies and similar online tracking tools?	Not Applicable
What do those laws or guidelines require for the use of cookies or similar online tracking tools?	There are no specific legal requirements under the PDPO for use of cookies or online tracking tools. See the PCPD's guidance on online behaviour tracking for best practices here.

Data sharing and engaging processors

Are there any requirements for sharing personal data or engaging third party data processors to process personal data?	Data subjects should be notified of the classes of recipients to whom personal data may be transferred to in accordance with DPP 1(3). See the response to question 3(2) on engaging data processors.

Data localization and cross-border transfer

Are there data localization or similar laws that require personal data to be retained in the local jurisdiction?	**None**. Section 33 of the PDPO contains a restriction on overseas transfers of personal data, but this has not yet come into force. The PCPD issued the Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data (see here), which provides a set of best practice contractual terms to be incorporated into agreements for the cross-border transfers of personal data on a "controller-to-controller" basis and a "controller-to-processor" basis.
What are legal mechanisms for cross-border data transfers ?	Not Applicable

Data subject rights

What are the data subject rights provided under the jurisdictions' data protection law?	**□ Right to be informed. What does this right require the organisation to do?** This is covered by the right to request access to personal data below. **□ Right of access. What does this right require the organisation to do?** Subject to any available grounds of refusal or exemptions, within 40 days of receiving a data access request ("**DAR**") from a data subject, the data user should inform the data subject whether it holds personal data of the data subject, and if so supply a copy of data to the data subject, or inform the data subject in writing that it does not hold such data. **□ Right to rectification. What does this right require the organisation to do?** A data subject may make a data correction request ("**DCR**") in relation to the personal data obtained by way of a DAR. Subject to any available grounds of refusal, within 40 days of receiving the DCR, if the data user discovers that the data being requested for correction is inaccurate, it should comply with the DCR and supply a copy of the corrected personal data to the data subject; if the data user is not satisfied that the personal data is inaccurate, it should give written notice and reasons for the refusal to the data subject.

Data protection impact assessments

In what circumstances are data protection impact assessments required?	There is no requirement under the PDPO for data users to conduct PIA, but this is advisable by the PCPD – see the PCPD's Information Leaflet on Privacy Impact Assessment here.

Data Protection Officer

Is there a requirement to appoint a DPO? If yes:	Not Applicable
In what	

circumstances is it required to appoint a DPO?	Not Applicable
Does the DPO have to possess certain qualifications or meet specific requirements? If so, what are these qualifications or requirements?	Not Applicable
What are the responsibilities of a DPO?	Not Applicable

Registration notification or filing requirements

Are there obligations to register with or notify the data protection authority in order to collect or process personal data generally?	Not Applicable

Security requirements and breach notification

What obligations does the jurisdiction's data protection law impose, with respect to maintaining security controls to protect personal data from unauthorized access?	Under DPP 4 of the PDPO, data users must take all practical steps to ensure that personal data is protected against unauthorised or accidental access, processing, erasure, loss or use, taking into account various factors such as the kind of personal data and the harm that could result.
How is a "data breach" or "data incident" defined?	

	The PDPO does not define "data breach" or "data incident", however the PCPD's Guidance on Data Breach Handling and Data Breach Notifications (see here). ("**Data Breach Guidance**") states that a data breach is generally regarded as a suspected or actual breach of the security of personal data held by a data user, which exposes the personal data of data subject(s) to the risk of unauthorised or accidental access, processing, erasure, loss or use.
Are there mandatory obligations on the steps an organization is required to take in the event of a data breach / incident?	Under the PDPO, there are no mandatory requirements in relation to the steps a data user is required to take in the event of a data breach or incident. However, the Data Breach Guidance recommends the following steps: immediate gathering of essential information relating to the breach; containing the data breach; assessing the risk of harm; considering giving data breach notifications; and documenting the breach.
Are there mandatory obligations to notify a regulator or data subjects about a personal data security breach?	Under the PDPO, there are no mandatory requirements to notify the data protection authority or impacted data subjects of data breach or data incident. However, the Data Breach Guidance encourages data users to make notification when a real risk of harm is reasonably foreseeable if no notification is made, and states that formal notification to affected data subjects and the authorities is appropriate where the affected data subjects could take proactive measures to reduce or mitigate the potential harm resulting from the breach, such as in cases where the data in question could be used to perpetrate identify theft or fraud.

DP authority and enforcement focus penalties under DP laws

Who is the main data privacy authority or regulator in your jurisdiction?	The PCPD.
What are the penalties for non-compliance with local data protection laws?	Under the PDPO, failure to comply with any of the DPPs is not a criminal offence in and of itself. However, if the PCPD investigates a complaint or suspected contravention of the PDPO, and finds that the data user is indeed contravening any of the DPPs, it may serve an enforcement notice. A failure to follow the enforcement notice is an offence, and the data user is liable: (i) on first conviction, to a fine of HK$50,000 and to imprisonment for 2 years and if the offence continues after the

conviction, a daily penalty of HK$1,000; and (ii) on a second or subsequent conviction, to a fine of HK$100,000 and to imprisonment for 2 years and if the offence continues after the conviction, a daily penalty of HK$2,000.

There are separate penalties for direct marketing offences and doxing offences, which attract a maximum fine of HK$1,000,000 and imprisonment of up to 5 years.

(a) Do data subjects have any private remedies?

Yes. Section 66 of the PDPO provides that an individual who suffers damage (which may be or include injury to feelings) by reason of a PDPO contravention by a data user may be entitled to compensation from that data user for that damage. The PCPD may, pursuant to section 66B of the PDPO, grant legal assistance to the aggrieved individual who intends to institute proceedings to seek compensation.

Has the data privacy regulator issued any notable enforcement guidance or judgments in the last 12-24 months?

Yes, the PCPD is active in enforcing the PDPO and regularly publishes enforcement, investigation and compliance check reports – see here.

Associated Contacts

Tommy Liu

Email Me

Kenneth Cheung

Email Me

Indonesia

Last updated 16 September 2025

Overview of Personal Data Protection Laws

What is the principal legislation, law or regulation governing personal data protection?	Law No. 27 of 2022 on Personal Data Protection ("PDP Law"), enacted in 2022 and fully effective as of 2024. The PDP Law has since been affected by the Constitutional Court Decision No. 151/PUU-XXII/2024, particularly for the Article 52 of PDP Law which governs requirements for the appointment requirements of a Data Protection Officer.
Do the jurisdiction's data protection laws have extra-territorial scope?	Yes, the PDP Law establishes an extraterritorial application, under which sets out that it applies to any individual, legal entity, public authority, or international organization, whether domiciled in Indonesia or abroad, where the relevant conduct: a. Gives rise to effects within the territory of Indonesia; and/or b. Affects Indonesian Personal Data Subjects outside the territory of Indonesia.

Key definitions under data privacy laws

What are the definitions of: (a) personal data, and (b) sensitive personal data under data protection laws?	**a. Provide examples to distinguish between "personal data" and "sensitive personal data."** (a) Personal data is defined as data regarding individuals who are identified or can be identified, either separately or in combination with other information, directly or indirectly through an electronic or non-electronic system. The PDP Law classifies personal data to "general personal data" and "specific personal data". General personal data includes: (i) full name; (ii) gender; (iii) citizenship; (iv) religion; (v) marital status; and/or (vi) combined personal data to identify a person (i.e., phone number and IP address). Further, specific personal data is defined as set out below. (b) Sensitive personal data is not explicitly defined in the PDP Law. However, the PDP Law recognizes "specific personal data", similar to those of "sensitive personal data" under EU GDPR, which is personal

	data that, when processed, may cause a greater impact on the personal data subject, including discriminatory treatment and greater damages to the subject. Specific personal data includes: (i) health data and information; (ii) biometric data; (iii) genetic data; (iv) criminal records; (v) child data; and/or (vi) personal financial data.
What (if any) exceptions apply to the above definitions of personal data or sensitive personal data?	The PDP Law does not apply to processing by a natural person for purely personal or household activities. Furthermore, certain data subject rights can be limited for national security, law enforcement, public interest in the context of state administration, or financial-system oversight.

Controller vs Processor

Do the jurisdiction's data protection laws include the concept of: (a) a "controller", and (b) a "processor"? How are they defined?	Yes. A controller means any person, public body, or international organization acting alone or jointly to determine the purposes of and exercise control over the processing of personal data. Meanwhile, a processor is any person, public body, or international organization acting alone or jointly to process personal data on behalf of a controller.
Do controllers have any legal obligations to control how processors manage the personal data that the controllers provide to them?	Not specifically. However, a data processor's conduct or processing activities is subject to data controller's instruction.

Legal basis for collection and processing

What are the legal bases permitting an	**□ Consent:** (a) What are the conditions or requirements for obtaining valid consent?

organization to collect and process personal data?

(a) What are the conditions or requirements for obtaining valid consent?

When relying on consent, the controller must provide the data subject with at least:

i. legality of the processing
ii. purpose of the processing
iii. types and relevance of data to be processed
iv. retention period for documents containing the data
v. details of information collected
vi. the period of processing
vii. the data subject's rights

In the case of obtaining the consent of personal data of children, the consent must be given by the parent and/or guardian. For persons with disabilities, the consent must be given by a person and/or guardian with appropriate communication methods

(b) Does the jurisdiction's data protection law recognise different types of consent?

Yes. A consent given by subjects may be in the form of writing or recording and either electronic or non-electronic. In substance, the consent must be explicitly given in simple and clear language by the subjects.

(c) Can consent be withdrawn?

Yes, it can. Data subjects have the right to withdraw consent, and upon withdrawal the controller must stop processing no later than 72 hours from the receipt of the request.

□ "Legitimate interests". If applicable –

What interests are considered legitimate interests?

- The PDP Law does not specify further what interests are considered as legitimate interest. However, it recognises legitimate interests as one of the lawful bases for personal data processing.
  For an organisation to rely on "legitimate interests", what are the relevant requirements or conditions?

- The PDP Law does not further outline what are the relevant requirements or conditions for the businesses to rely on legitimate interests. However, in practice, many businesses

conduct the purpose, necessity, and balancing tests extracted from the practices of EU and UK GDPR.

- **"Contractual necessity". If applicable –**
  - **What purposes would fall under this legal basis?**

    The PDP Law recognizes contractual necessity as a legal basis for processing personal data. It is defined as any processing of a personal data for the fulfilment of agreement obligations if a personal data subject is a party to, or to fulfil the request of personal data subject at the time into entering into the agreement.

  - **For an organisation to rely on this legal basis, what are the relevant requirements or conditions?**

    There are no specific requirements or conditions to rely on this legal basis set out in the PDP Law.

- **"Compliance with legal / regulatory requirement". If applicable –**
  - **What purposes would fall under this legal basis?**

    Although recognised, PDP Law does not specify further on this topic.

  - **For an organisation to rely on this legal basis, what are the relevant requirements or conditions?**

    There are no specific requirements or conditions to rely on this legal basis set out in the PDP Law.

- **Other legal basis apart from the above. If applicable –**
  - **What are the other legal bases?**
    - The fulfilment of the protection of vital interests of the personal data subject; and
    - Carrying out duties in the context of public interest, public services, or exercising the authority of the controller based on laws and regulations.
  - **What purposes would fall under each legal basis**

mentioned above in 5.a?

- What is meant by 'vital interests of the data subject' is related to the survival of the personal data subject (i.e., when the processing of personal data is necessary for serious medical treatment).
- 'Public interest, public services, or exercising the authority of the controller based on laws and regulations' is not elaborated further in the PDP Law as it is self-explanatory.

- **For an organisation to rely on each legal basis mentioned above in 5.a, what are the relevant requirements or conditions?**

There are no specific requirements or conditions to rely on the legal basis above set out in the PDP Law.

If local law recognizes the concept of "sensitive" personal data, are there special rules to the legal bases mentioned in Q.1, or different legal bases than the above, for an organization to collect or process sensitive personal data?

Please see our response in 2.1.(b). There are no different legal bases for the collection or processing of specific personal data.

- What are the special rules / different legal bases?

Not applicable.

- For an organisation to rely on each legal basis mentioned above in 6.a, what are the relevant requirements or conditions?

Not applicable.

Transparency / disclosure requirements

Are there any transparency or disclosure requirements under the jurisdiction's data protection laws, requiring disclosure of certain information to

Please see our response in 4.a above.

data subjects? If yes – What are the items of information that must be disclosed to data subjects?	
Are organizations required to have a privacy policy? If yes, must the privacy policy cover the information as in the 'Overview of Personal Data Protection Laws' above, or is any additional information required to be covered?	PDP Law does not expressly require organizations to publish a document titled privacy policy. However, the disclosure duties above apply, including the duty to inform data subjects before changing key information and the general transparency principle. In practice, a written privacy notice or policy should cover the mandatory items in 4.a above and support the access and record obligations.

Data of children or minors

Are there specific laws, regulations, rules or guidelines that govern the collection or processing of children's personal data?	Yes. Children's personal data is categorized as "specific personal data", in which to process a child's personal data, prior consent from the child's parent and/or guardian is required.
What mandatory requirements do those laws, regulations, rules or guidelines provide for the collection or processing of children's personal data?	a. **If consent applies in respect of collecting or processing children's personal data, what constitutes valid consent?** In addition to the consent from the child's parent and/or guardian, please see our response in 4.a above.

Direct and e-marketing online tracking and cookies requirements

What constitutes direct marketing	PDP Law is silent on this matter. As direct marketing pertains to the use of users' personal data, please see below the requirements.

under the jurisdiction's data protection laws?	
What are the requirements for the use of personal data for direct marketing or e-marketing?	◦ **Consent. What are the consent requirements specific to direct marketing or e-marketing?** There are no specific requirements to direct marketing or e-marketing, thus the general requirement of consent applies as per our response in 4.a above. ◦ **Disclosure. What are the requirements for disclosing information to data subjects which are specific to direct marketing or e-marketing?** N/A ◦ **Other requirements. What are the other requirements specific to direct marketing or e-marketing?** N/A
What specific laws, regulations or guidelines (if any) govern the use of cookies and similar online tracking tools?	There are no specific laws, regulations, or guidelines that govern the use of cookies and similar online tracking tools in Indonesia. Thus, the general requirements for personal data processing shall apply.
What do those laws or guidelines require for the use of cookies or similar online tracking tools?	Not Applicable

Data sharing and engaging processors

Are there any requirements for sharing personal data or engaging third party data	Yes, please see our response in point 4 above.

processors to process personal data?

Data localization and cross-border transfer

Are there data localization or similar laws that require personal data to be retained in the local jurisdiction?	Data localisation requirements only apply for data controller categorised as a Public Electronic System Provider i.e. appointed by the government for the processing of personal data for public purposes. While for businesses, provided that it did not appointed by the government as aforementioned, this requirement does not applies. As for cross-border data transfer, please see our response below.
What are legal mechanisms for cross-border data transfers ?	☐ Data subject consent ☐ Transfers to jurisdictions which are whitelisted or subject to an adequacy decision ☐ Standard data protection clauses (SCCs) ☐ Binding corporate rules (BCRs) ☐ Codes of conduct ☐ Certification mechanisms ☐ Ad hoc contractual clauses ☐ Approval from or registration or filing with local authorities Please see our response below. ◦ **For each of the applicable mechanisms, what are the requirements for the organisation seeking to transfer personal data to rely on such mechanism?** Please note that the data controller must ensure compliance with the cross-border transfer requirements under the PDP Law, i.e.: ◦ the destination country must have a level of personal data protection that is equal to or higher than the level mandated under the PDP Law; or ◦ if the first condition is not met, the recipient in the destination country must be bound by adequate and enforceable personal data protection safeguards; or ◦ if neither condition is fulfilled, explicit consent of the relevant personal data subject for the cross-border

transfer shall first be obtained.

The above requirements were extracted from the draft implementing regulation of the PDP Law, which is currently being finalized by the Indonesian government and is expected to be enacted in the near future. At present, the PDP Law itself does not provide further elaboration on the technicalities of cross-border personal data transfers.

- **What if any derogations are permitted by law?**

The express derogation is reliance on the data subjects' consent when the adequacy test and the adequate and binding safeguards condition cannot be satisfied.

Data subject rights

What are the data subject rights provided under the jurisdictions' data protection law?

□ Right to be informed. What does this right require the organization to do?
Please see our response in 4.a above.

□ Right of access. What does this right require the organization to do?
Provide access and a copy of the data subjects personal data no later than 72 hours as of receiving data subject's request to access.

□ Right to rectification. What does this right require the organization to do?
Grant data subject's request to correct and/or update inaccurate personal data no later than 72 hours as of receiving data subject request.

□ Right to erasure. What does this right require the organization to do?
Grant data subject's request to erase the processed personal data. No specific timeline available.

□ Right to restrict processing. What does this right require the organization to do?
Grant data subject's request to delay or limit the processing of personal data in a proportionate manner consistent with the processing purpose. No specific timeline available.

□ Right to data portability. What does this right require the

organization to do?
Provide the data subject with their personal data in a structure or format commonly used or readable by electronic systems, and to enable the data subject to use and send their personal data to another controller where systems can securely intercommunicate. No specific timeline available.

Right to object. What does this right require the organization to do?
Receive and handle objections against decisions that are based solely on automated processing including profiling where such decisions produce legal effects or significantly affect the data subject.

Rights related to automated decision-making including profiling. If applicable, what does this right require the organization to do?
Same as immediately above, the data subject may object to decisions based only on automated processing including profiling that have legal or significant effects. No specific timeline available.

Data protection impact assessments

In what circumstances are data protection impact assessments required?	A personal data protection impact assessment is required when the processing poses a potential high risk to data subjects. High risk includes automatic decision making that has legal or significant effects on data subjects, processing of specific personal data, large scale processing, systematic evaluation or scoring or monitoring of data subjects, matching or combining datasets, use of new technology, and processing that restricts data subject rights. This includes the evaluation of potential risks arising from the processing and the steps to mitigate those risks, including impacts on data subject rights and compliance.

Data Protection Officer

Is there a requirement to appoint a DPO? If yes:	Yes.
In what circumstances is it required to	Data controller and data processor are required to appoint DPO in the event that:

appoint a DPO?	a. the processing of personal data are for the benefit of public services b. the core activities of the data controller have the nature, scope, and/or purposes that require regular and systematic monitoring of personal data on a large scale; and/or c. the core activities of the data controller consist of the personal data processing on a large scale for specific personal data and/or personal data related to crimes. If one of the abovementioned requirements is met, DPO is mandatory to be appointed.
Does the DPO have to possess certain qualifications or meet specific requirements? If so, what are these qualifications or requirements?	Yes. Generally the PDP Law outlines that the DPO shall be appointed based on professionalism, knowledge of the law, personal data protection practice, and ability to fulfil their duties.
What are the responsibilities of a DPO?	Officials or officers who carry out the personal data protection function as a DPO have at least the following duties: a. inform and provide advice to the personal data controller or the personal data processor in order to comply with the provisions of this law; b. monitor and ensure compliance with this law and the policies of the personal data controller or personal data processor; c. provide advice on assessing the impact of personal data protection and monitoring the performance of the personal data controller and the personal data processor; and d. coordinate and act as a liaison for issues related to the processing of personal data.

Registration notification or filing requirements

Are there obligations to register with or notify the data protection authority in order to collect or process personal data generally?	Not Applicable

Security requirements and breach notification

What obligations does the jurisdiction's data protection law impose, with respect to maintaining security controls to protect personal data from unauthorized access?	a. Implement and maintain technical and operational measures to secure personal data, and set an appropriate security level having regard to the nature and risks of the data being processed. b. Maintain the confidentiality of personal data during processing. c. Supervise every party involved in the data processing under the controller's control. d. Protect personal data from unlawful processing. e. Prevent unauthorized access by using a security system for the data processed and or by processing through electronic systems that are reliable, safe, and responsible, in accordance with regulations.# f. For high-risk processing, perform a personal data protection impact assessment to identify and mitigate risks, including where processing is automated with legal or significant effects, involves specific data, is large scale, uses new technology, or limits data subject rights. g. When transferring personal data, both the sending and receiving controllers must ensure data protection as required by the Law, and for cross border transfers the controller must ensure an equivalent or higher level of protection or put adequate and binding safeguards in place.
How is a "data breach" or "data incident" defined?	PDP Law defines data breach as failure to protect a person's personal data in respect of confidentiality, integrity, and availability, including a security breach whether intentional or unintentional, that leads to destruction, loss, alteration, disclosure, or unauthorised access to personal data that is transmitted, stored, or processed.
Are there mandatory obligations on the steps an organization is required to take in the event of a data breach / incident?	Yes. In the event of an incident occurs, the data controller is required to provide written notification within 72 days to both the data subject and the regulator (currently, the Ministry of Communications and Digital ("MOCD") as the transitional authority).
Are there mandatory obligations to notify a regulator or data subjects about a personal data security breach?	**When is a notification obligation triggered:** □ Quantitative threshold (e.g. volume of data or number of data subjects involved) – [set out the threshold] □ Qualitative threshold (e.g. sensitivity of data or risk posed to data subjects) – [set out the threshold] Currently, the threshold is when the data breach affects the confidentiality, integrity, and availability of personal data, including a

security breach whether intentional or unintentional, that leads to destruction, loss, alteration, disclosure, or unauthorised access to personal data that is transmitted, stored, or processed.

What is the timing requirements for making a notification?

Written notification must be given no later than 72 hours as of the data controller has duly known/identified the breach.

What content must the notification contain?

The notification must at least state the personal data disclosed, when and how the disclosure occurred, and the measures taken by a controller to handle and recover from the disclosure. In certain conditions, the controller must also notify the public, which shall mean situations where the failure interferes with public services and or has a serious impact on the public interest.

Are there any other requirements for making notifications?

The notification form for regulator, i.e. MOCD, is only available in Indonesian language, while there is no format for notification to data subject. Commonly acceptable approach is that all of the notifications to be also made available in Indonesian language.

DP authority and enforcement focus penalties under DP laws

Who is the main data privacy authority or regulator in your jurisdiction?

PDP Law mandates that the main authority is a Personal Data Protection Agency which is yet to be established as of the date of this questionnaire.

Currently, MOCD serves as transitional authority to oversee the implementation of PDP Law in Indonesia.

What are the penalties for non-compliance with local data protection laws?

a. **Certain violations of the PDP Law may trigger administrative sanctions in the form of:**
    - Written warning.
    - Temporary suspension of personal data processing activities.
    - Deletion or destruction of personal data.
    - Administrative fine up to 2 percent of annual income or annual revenue, imposed by the authority; further procedures to be set by government regulation.

b. **Certain violations of the PDP Law may trigger criminal sanctions as below:**
    - Unlawful obtaining or collecting personal data with intent to benefit oneself or another that may cause loss to the data subject: up to 5 years imprisonment and/or fine up to IDR 5,000,000,000.
    - Unlawful disclosure of personal data not one's own: up to 4 years imprisonment and/or fine up to IDR 4,000,000,000.
    - Unlawful use of personal data not one's own: up to 5 years imprisonment and/or fine up to IDR 5,000,000,000.
    - Creating or falsifying personal data to benefit oneself or another, causing loss to others: up to 6 years imprisonment and/or fine up to IDR 6,000,000,000.
    - Additional criminal punishments may include confiscation of proceeds or assets derived from the offence and payment of compensation.
      If the offence is committed by a corporation, punishment may be imposed on the management, controlling party, person giving the order, beneficial owner, and or the corporation. The primary penalty for a corporation is a fine, up to 10 times the maximum fine otherwise applicable. In addition, the court may order:
        - Confiscation of proceeds or assets;
        - Freezing of all or part of the business;
        - Permanent prohibition from certain acts;
        - Closure of all or part of premises or corporate activities;
        - Performance of neglected obligations;
        - Payment of compensation;
        - Licence revocation; and or
        - Dissolution of the corporation.

c. **Do data subjects have any private remedies?**
Yes.

Data subjects are entitled to lodge a civil claim and receive compensation for any violations towards the processing of their personal data.

Has the data privacy regulator issued any notable enforcement guidance or judgments in the last 12-24 months?	No. However, the Indonesian government plans to issue a technical implementing regulation of PDP Law in the near future.

Associated Contacts

Mochamad Kasmali

Email Me

Teguh Darmawan

Email Me

Andera Rabbani

Email Me

Japan

Last updated 18 September 2025

Overview of Personal Data Protection Laws

What is the principal	The principal data protection legislation in Japan is the Act on the Protection of Personal Information ("**APPI**").

legislation, law or regulation governing personal data protection?	
Do the jurisdiction's data protection laws have extra-territorial scope?	Yes, the APPI is applicable to data handlers (defined below) located overseas that handle personal information related to individuals in Japan, in relation to supplying goods or services to individuals in Japan. (APPI, Article 171)

Key definitions under data privacy laws

What are the definitions of: (a) personal data, and (b) sensitive personal data under data protection laws?

a. Provide examples to distinguish between "personal data" and "sensitive personal data."

Under the APPI, "personal information" and "personal data" are defined separately.

- "Personal information" is defined as information relating to a living individual that falls under any of the following items: (i) information containing a name, date of birth, or other identifier or their equivalent that can be used to identify a specific individual (meaning any and all such items of information (excluding individual identification codes) made by writing, recording, sound or motion, or other means, in a document, drawing, or electronic or magnetic record; and (ii) information containing individual identification codes. (APPI, Article 2)
- "Personal data" is defined as "personal information compiled in a personal information database or its equivalent." (APPI, Article 16)

Sensitive personal information (APPI, Article 2)

- "Sensitive personal information" is defined as personal information referring to an identifiable person's race, creed, social status, medical history, criminal record, the fact of having suffered damage by a crime, or other identifiers or their equivalent prescribed by Cabinet Order as those of requiring special care so as not to cause unjust discrimination, prejudice or other disadvantages to that person.

What (if any) exceptions apply to the above definitions of personal data or sensitive personal data?	Not applicable

Controller vs Processor

Do the jurisdiction's data protection laws include the concept of: (a) a "controller", and (b) a "processor"? How are they defined?	No, the APPI does not recognise the concepts of, nor make distinctions between, "data processors" and "data controllers". However, the APPI defines a "Business Handling Personal Information" (APPI, Article 16) as a person that uses a personal information database or its equivalent for business (excluding governments or other certain public sectors) ("**data handler**"). The data handler under the APPI may include both concepts of data controllers and processors.
Do controllers have any legal obligations to control how processors manage the personal data that the controllers provide to them?	Data handlers have the obligation to exercise necessary and adequate supervision over persons to whom they entrust the handling of personal data (similar to data processor) so as to ensure the secure management of such personal data. (APPI, Article 25)

Legal basis for collection and processing

What are the legal bases permitting an organization to collect and process personal data?	**Consent:** (a) What are the conditions or requirements for obtaining valid consent? • Please note that a legal basis to collect or process personal data is not required under the APPI. However, there are other obligations imposed on the data handler to protect personal data. For example, to collect sensitive personal information, a data handler must obtain consent from data subjects at the time of collection in general unless an exception applies (APPI, Article 20). Further consent is generally required for a third-

party transfer ("**General Transfer**") and/or an international transfer ("**International Transfer**") of personal data (APPI, Articles 27, 28, etc.; see Sections 8 and 9 below for more details) unless an exception for each relevant transfer applies. These consents can be obtained at once, for example, by obtaining consent to a privacy policy stipulating transfer conditions.

For sending marketing emails, prior consent is generally required (Opt-in). (See Section 7 below for more details)

- The valid consent under the APPI means recognizing the individual's expression of intent to consent. Depending on the nature of the business and the circumstances surrounding the handling of personal information, reasonable and appropriate methods deemed necessary for the individual to make a decision regarding consent must be employed. The following are examples of ways to obtain valid consent:
    - Verbal expression of consent by the individual
    - Receipt of a written statement (including electronic records) from the individual indicating consent
    - Receipt of an email from the individual indicating consent
    - Checking a box by the individual indicating consent
    - Clicking a button on a website by the individual indicating consent
    - Voice input, touch panel input, button or switch input, etc., by the individual indicating consent

(b) Does the jurisdiction's data protection law recognise different types of consent?

Consent can be implied or express, depending on the circumstances.

(c) Can consent be withdrawn?

No. Under the APPI, there are no rules explicitly entitling data subjects to withdraw consent, although the data handler's acceptance of such withdrawal in handling personal information is practically recommended.

Note: Instead, the data subject may request deletion, cessation of use or cessation of transfer to a third party of his/her personal information subject to conditions based on the data subject's rights (see Section 10 below).

Other legal basis apart from the above:

a. What are the other legal bases?

As mentioned above, a legal basis to collect or process personal information is not required under the APPI. However, data handlers are restricted by the rules below, for example:

- The data handler must not:
  - use personal information beyond the scope necessary to achieve the specified utilization purposes (APPI, Article 18);
  - utilize personal information in a way that has the possibility of fomenting or inducing an unlawful or unjust act (APPI, Article 19); or
  - acquire personal information by deception or other wrongful means (APPI, Article 20).
- Regarding consent requirement for collecting sensitive personal information, data handlers may obtain sensitive personal information without obtaining consent in the following cases, for example (APPI, Article 20):
  - When required by a law in Japan
  - When necessary to protect human life, physical safety, or property, and obtaining the individual's consent is difficult.
  - When particularly necessary for the improvement of public health or the sound development of children, and obtaining the individual's consent is difficult.
  - When it is necessary to cooperate with a national agency, local public entity, or a person commissioned by such an entity in the performance of duties prescribed by a law in Japan, and obtaining the individual's consent would likely hinder the performance of such duties.
  - When the data handler is an academic research institution or its equivalent, and it is necessary to handle or collect the

	sensitive personal information for academic research purposes excluding cases in which there is a risk of unjustly infringing on individual rights and interests. ◦ When the sensitive personal information is acquired from an academic research institution or its equivalent and it is necessary to acquire that information for academic research purposes (limited to cases in which the data handler and the academic research institution or its equivalent jointly conduct academic research); ◦ When the sensitive personal information is open to the public by a person identifiable by that information, a national government organ, a local government, an academic research institution; or ◦ their equivalent as specified under the APPI rules.
If local law recognizes the concept of "sensitive" personal data, are there special rules to the legal bases mentioned in Q.1, or different legal bases than the above, for an organization to collect or process sensitive personal data?	Not applicable

Transparency / disclosure requirements

Are there any transparency or disclosure requirements under the jurisdiction's data protection laws, requiring disclosure of	◦ Data handlers must make the following information about the personal data they hold ("Holding Data") accessible to identifiable persons, for example (APPI, Article 32): ◦ the name and address of the business handling personal information, and if it is a corporation, the name of its representative (i.e. CEO, not DPO):

certain information to data subjects? If yes – What are the items of information that must be disclosed to data subjects?

- the purpose of use; and
- the procedures for responding to a data subject's request.

- If the purpose of use regarding the personal information has not been disclosed in advance, a data handler must promptly notify the individual of the purpose of use or make it public (APPI, Article 21).
- Further, when obtaining consent, appropriate disclosure of information is required such as in the case of obtaining consent for International Transfers (APPI, Article 28).

Are organizations required to have a privacy policy? If yes, must the privacy policy cover the information as in the 'Overview of Personal Data Protection Laws' above, or is any additional information required to be covered?

Practically yes, although the APPI does not explicitly require a data handler to have a privacy policy.

As mentioned above, the APPI has disclosure requirements and the requisite information is disclosed via a privacy policy as a matter of practice and this practice is generally most appropriate.

Data of children or minors

Are there specific laws, regulations, rules or guidelines that govern the collection or processing of children's personal data?

The APPI does not include provisions explicitly governing the collection or processing of children's personal data specifically at this moment.

However, recently, there has discussions about introducing new rules regarding this matter so we should keep an eye on further developments.

What mandatory requirements do those laws, regulations, rules or guidelines provide for the collection or

As noted above, no special rules apply to minors specifically under the APPI, at least for now. Handling children's personal data must comply with the same laws as those for adults.

(a) If consent applies in respect of collecting or processing children's personal data, what constitutes valid consent?

processing of children's personal data?

Where consent is required, for that consent to be valid, the individual must have capacity to consent. The Q&A of the APPI Guidelines issued by the Personal Information Protection Commission ("**PPC**") suggests that, generally, the data handler must obtain parental (or guardian) consent when collecting or processing personal data of children that are under 12-15 years old depending on the specific circumstances such as the specific items of personal information handled or the nature of the occasion.

Direct and e-marketing online tracking and cookies requirements

What constitutes direct marketing under the jurisdiction's data protection laws?

The APPI does not define "direct marketing" and ordinary rules under the APPI apply.

In the meantime, generally, marketing communications in Japan are subject to the *Act on Specified Commercial Transactions* (Act No. 57 of June 4, 1976, as amended; "**ASCT**") to protect consumers and The *Act on the Regulation of Transmission of Specified Electronic Mail* (Act No. 26 of 2002, as amended; "**Anti-Spam Act**") to protect cyber space.

What are the requirements for the use of personal data for direct marketing or e-marketing?

 Consent. What are the consent requirements specific to direct marketing or e-marketing?

- **ASCT:**
  The ASCT restricts marketing emails related to online sales, teleshopping, mail-order sales and other similar sales methods to consumers (collectively "**Online Sales**"). A company engaging in such Online Sales activities must comply with the ASCT.

  The ASCT generally prohibits a seller from sending email or fax advertisements (including text messages, email, and push notifications) to consumers unless they provide prior request or consent (i.e. opt-in requirement). The seller may be exempted from this opt-in requirement only where one of specific exceptions applies (e.g. parties are in the course of business, advertisement is supplementary). Also, a seller is required to retain records that show the consumers' request or consent to receive email or fax advertisements for three years from the date of sending marketing email.

- **Anti-Spam Act**
  The Anti-Spam Act regulates emails and short messages (i.e. messages transmitted via a service that sends and receives messages via telephone numbers including text messages, email, and push notifications) sent as a means of advertising or promoting business ("**Marketing Email**"). The sender of such Marketing Email is subject to the requirements below unless one of specific exceptions applies (e.g. advertisement is supplementary):
    - **Opt-in:** The sender may only send the Marketing Email to those who have agreed to receive Marketing Emails. The sender must keep a record showing the circumstances under which consent was given for one month from the last date of sending Marketing Emails.The sender must not send Marketing Emails falsifying the email address or telecommunication facilities for sending Marketing Email.**Opt-out**: If the sender receives a notice of refusal to receive Marketing Emails, it must not send any further emails.

The sender must prepare a measure for enabling the user to opt-out and state the measure in the Marketing Email including certain information (see "Disclosure" section below).

 Disclosure. What are the requirements for disclosing information to data subjects which are specific to direct marketing or e-marketing?

- Generally, Marketing Emails must include the following information (Opt-out function under the Anti-Spam Act);
    - who the sender is;
    - a notification that the customer has the ability to opt-out;
    - a description of how to opt-out (e.g. email address or URL);
    - the address of the responsible person; and
    - contact information to complain or ask questions (e.g. telephone number, email address or URL).
- Disclosure requirements for Online Sales

If the entity conducts Online Sales to consumers, the entity should comply with the requirements under the ASCT, for example:

i. Inform consumers of certain information on sales such as the name of their business and the purpose of the solicitation before starting solicitation; and
ii. Provide a document detailing important matters at the time of contract conclusion.

 Other requirements. What are the other requirements specific to direct marketing or e-marketing?

The provision of promotional materials or free merchandise to customers may be prohibited subject to conditions (e.g. exceeding the price limit) under the *Act against Unjustifiable Premiums and Misleading Representations* (Act No. 134 of May 15, 1962, as amended; "**APR**") The APR also prohibits misleading representations in advertisements such as where the quality, standard or any other particular relating to the content of goods or services is portrayed to general consumers as being significantly superior to that of the actual goods or services etc.; or by which the price or any other trade terms of goods or services could be misunderstood to be significantly more advantageous than the actual goods or services supplied, etc.

What specific laws, regulations or guidelines (if any) govern the use of cookies and similar online tracking tools?

Telecommunications Business Act (Act No. 70 of 2022, as amended; "**TBA**") and APPI

What do those laws or guidelines require for the use of cookies or similar online tracking tools?

- TBA - External Transmission Regulations (so-called cookie rules)
  TBA, Article 27-12
  When using websites or apps, if user information is transmitted to a third party without the users' consent, measures must be implemented to ensure that the users can check this themselves. The TBA requires telecommunication business operators (this concept is relatively broad, including operators of chat, email, search engine services, subject to conditions) to notify users in general of, or make accessible to users in general:
  - the types of user information to be transmitted;
  - the name of any recipients that will handle the user

information; and

- the purposes of use of all such user information.

The exceptions to such disclosure/notification requirement are as follows.

- The user information collected is required for the provision of service that the user wishes to use such as OS information, language setting, browser information, information to identify users, information required for security, administration of network, etc.
- The user information collected is identification codes stored in first party cookies that the entity sends to the user.
- Consent to such transfer is obtained in advance (note that opt-in consent is an exception, but is not necessary, for example, if the disclosure requirements above are satisfied.)
- Opt-out measures are prepared, and specific information is provided such as the fact that an opt-out measure has been implemented and details of the transfer of user information.

- APPI – restriction over "Information related to personal information ("**IPI**")"

This restriction applies only if the transferor knows the data recipient will use the information as personal information.

Under the APPI, IPI is defined as information from which a transferor is unable to identify a data subject based on such information alone, but from which a data recipient that receives such information from the transferor may be able to identify the data subject based on such information together with other information that is available to the data recipient (APPI, Article 2). The data handler (i.e. transferor) must confirm that the data recipient has obtained consent from the data subject to receive such IPI for usage as personal information (APPI, Article 31).

Data sharing and engaging processors

Are there any requirements for sharing personal data or engaging third party data processors to process personal data?	Under the APPI, to transfer personal data to a third party (including affiliates, vendors), regardless of whether the transfer is international or local, in principle, consent from a data subject is required (i.e. consent requirement for General Transfers) unless one of the exceptions (e.g. entrustment, joint-use) applies. (APPI, Article 27)

Data localization and cross-border transfer

Are there data localization or similar laws that require personal data to be retained in the local jurisdiction?	No, there is no overarching law that requires personal information to be stored or remain within the Japanese territory. Data handlers subject to the APPI are allowed to host or transfer data overseas, so long as they comply with the cross-border data protections rules and any other APPI requirements.
What are legal mechanisms for cross-border data transfers ?	☐ Data subject consent ☐ Transfers to jurisdictions which are whitelisted or subject to an adequacy decision ☐ Standard data protection clauses (SCCs) ☐ Binding corporate rules (BCRs) ☐ Codes of conduct ☐ Certification mechanisms ☐ Ad hoc contractual clauses ☐ Approval from or registration or filing with local authorities **(a) For each of the applicable mechanisms, what are the requirements for the organisation seeking to transfer personal data to rely on such mechanism?** In principle, it is necessary to obtain the data subject's consent to the transfer of his/her personal information to a data recipient located in a foreign country (including affiliates, vendors) under the APPI ("**International Transfer**"), unless one of the exceptions to this requirement applies (APPI, Article 28). ◦ As of September 2025, countries in the EEA and the UK are whitelisted regarding the consent requirement for International Transfers based on the Japan-EU mutual adequacy arrangement.

- If personal data is transferred to a data recipient that has in place a system conforming to adequate standards under the APPI, this would be another exception to the consent requirement for International Transfers. According to the PPC's Guidelines, the form may be, for example, (a) the execution of a data transfer / processing agreement conforming with the APPI's requirements e.g. with business partners, (b) establishment of BCRs, Codes of conduct e.g. among group entities or affiliates, or (c) qualification or recognition under an acceptable global privacy framework (e.g. certificate under the APEC CBPR system).
  In case of obtaining consent for International Transfers, certain information (e.g. jurisdictions of the recipient, outline of the data protection system of the recipient's jurisdiction) must be provided in advance (APPI, Article 28). As this requirement is somewhat complicated, we generally try to avoid this pathway.

  In case of using the exception to the consent requirement for International Transfers based on the data recipient establishing a system conforming to adequate standards, certain information must be provided to a data subject upon request of the data subject. The information that must be disclosed in this includes, for example, the measures established to ensure that the third party recipient satisfies the required APPI data protection standards; the country in which the third party is located; any obstacles or any system in the country of the third party recipient that may adversely affect the implementation of such measures and preventive measures taken against such obstacles, etc.

(b) What if any derogations are permitted by law?

The following are examples of cases that fall under further exceptions to the consent requirement for transfers of personal data: (APPI, Articles 28, 27):

1. transfers based on laws and regulations in Japan;
2. transfers that are necessary to protect the life, wellbeing, or property of an individual, where it is difficult to obtain the consent of the data subject;
3. transfers that are especially necessary to improve public wellbeing or promote healthy child development, where it is difficult to obtain the consent of the data subject;
4. transfers that are necessary to cooperate with a national

government organ, local government, or person entrusted thereby with performing the functions prescribed by laws and regulations in Japan, where obtaining the consent of the data subject is likely to interfere with the performance of those functions.

5. cases in which the data handler is an academic research institution or its equivalent, and providing the personal data for the purpose of publication of academic research results or teaching is unavoidable (excluding cases in which there is a risk of unjustly infringing on individual rights and interests);
6. cases in which the data handler is an academic research institution or its equivalent, and the provision of the personal data is necessary for academic research purposes (limited to cases in which the data handler and the third party jointly conduct academic research); and
7. cases in which the third party is an academic research institution or its equivalent, and the handling of the personal data by the third party is necessary for academic research purposes.

Data subject rights

What are the data subject rights provided under the jurisdictions' data protection law?

□ Right to be informed. What does this right require the organization to do?A data handler that handles Holding Data (similar to the concept of "data controller") generally has an obligation to make available to a data subject information in respect of the following items (APPI, Article 32).

i. name and address of the data handler (also the name of the representative (e.g. CEO) in case it is a legal entity);
ii. utilization purposes of Holding Data;
iii. information related to international transfer of data to third party in a country other than the EEA or the UK; and
iv. implemented measures for data security (except when such disclosure possibly impairs data security).

□ Right of access. What does this right require the organization to do?

A data subject may generally request that the data handler that handles Holding Data to disclose (a) Holding Data, and/or (b) transfer records of receiving and providing data required under the APPI (APPI, Article 33). The data handler must disclose the Holding Data/ transfer records in respect of that data subject without delay subject to some exceptions such as:

i. disclosure is likely to harm the life, wellbeing, property, or other rights or interests of the identifiable person or a third party;
ii. disclosure is likely to seriously interfere with the proper

implementation of the business of the data handler; or

iii. disclosure would violate any other law or regulation.

□ Right to rectification. What does this right require the organization to do?

A data subject may generally request the data handler that handles Holding Data relating to the data subject to correct, delete, or supplement the Holding Data, unless the content of the Holding Data subject to the request for rectification is factually correct/true. (APPI, Article 34)

The data handler must give notice to the data subject in the event,

i. the data handler makes a correction, deletion, or supplementation of the Holding Data relating to the data subject; or
ii. the data handler decides not to make a rectification.

□ Right to erasure. What does this right require the organization to do?

Please see the description above on the right to rectification covering the request to "delete" in this section (APPI, Articles 34 and 35).

□ Right to restrict processing. What does this right require the organization to do?

A data subject may generally request the data handler that handles Holding Data relating to the data subject to cease utilization of the Holding Data or delete the Holding Data under certain circumstances (APPI, Article 35):

- - in case of (a) a certain illegal collection or (b)improper usage under the APPI, or (c) usage beyond the notified purposes of use; or
  - if there is (a) no reason to use the data anymore, (b) a serious data breach incident or (c) some other risk of violating individual rights or legitimate interests.

  If the data handler receives a request to cease utilization or delete the Holding Data, it must investigate and address the request from the data subject without delay.

- A data subject may request the data handler that handles Holding Data relating to the data subject to cease transfer of the Holding Data to a third party under certain circumstances (APPI, Article 35):
  - where there is a certain illegal transfer under the APPI

(e.g. without consent); or

- if there is (a) no reason to use the data anymore, (b) a serious data breach incident or (c) some other risk of violating individual rights or legitimate interests.

If the data handler receives a request to cease transfer of the Holding Data, it must investigate and address the request from the data subject without delay.

Right to data portability. What does this right require the organization to do?
The APPI does not specifically address the right to data portability. However, the data subject may generally request information in a digital format under the right of access as described above. (APPI, Article 33)

Data protection impact assessments

In what circumstances are data protection impact assessments required?	While recommended as a practical matter, it is not a requirement under the APPI to conduct a privacy impact assessment.

Data Protection Officer

Is there a requirement to appoint a DPO? If yes:	No, in general.
In what circumstances is it required to appoint a DPO?	There is no requirement to appoint a DPO under the APPI, but it is recommended as a part of the implementation of security management measures. Further, the appointment of a DPO may be required for data handlers in some special business sectors (e.g. financial sector, certain telecommunications carriers).
Does the DPO have to possess certain qualifications or meet specific	No. However, practically, the DPO should have sufficient knowledge of data protection and data privacy practices in Japan.

requirements? If so, what are these qualifications or requirements?	Please note that for the finance sector, generally, the lead of DPOs must be the CEO or other executive officer who holds responsibility for business operations.
What are the responsibilities of a DPO?	◦ In the finance sector, two types of DPOs are generally required. ◦ Lead of DPOs who holds overall responsibility for executing tasks related to the secure management of personal data. ◦ DPOs assigned to each department that handles personal data. ◦ The DPO of certain telecommunications carriers is responsible for the following matters, for example: i. Formulate and submit regulations (internal rules) for handling specific user information. ii. Establish and publicly disclose policies for handling specific user information. iii. Conduct an annual self-assessment of the handling of specific user information and reflect the results in the regulations and handling policies.

Registration notification or filing requirements

Are there obligations to register with or notify the data protection authority in order to collect or process personal data generally?	There is no general legal requirement to register data processing activities nor a requirement to notify the PPC before collecting or processing personal data. However, the Opt-out system, which can be used as a means to forgo obtaining prior consent for General Transfers, requires filing with the PPC a privacy policy that is available to data subjects including sufficient information under the APPI (APPI, Article 27).

Security requirements and breach notification

What obligations does the jurisdiction's data protection law impose, with respect to	The APPI does not provide specific security measures that must be established (although the PPC guidelines provide various detailed recommendations for implementing these measures), but a data handler must take necessary and appropriate measures for managing the

maintaining security controls to protect personal data from unauthorized access?	security of personal data including preventing the leakage, loss or damage of the personal data they handle (APPI, Article 23). The degree of compliance is judged based on the totality of circumstances. Further, a data handler has the obligation to exercise adequate supervision, in light of data security, over its employees (APPI, Article 24) and persons to whom the data handler entrusts the handling of personal data (e.g. contractors, entrustees) (APPI, Article 25)
How is a "data breach" or "data incident" defined?	The APPI does not define the term "data breach" or "data incident". However, a data handler has a reporting obligation in general where there is a leakage, loss, damage or other situation concerning the insurance of security of its handled personal data including where there is a risk of these situations occurring or having occurred (collectively "**Leakage and its equivalent**"). (APPI, Article 26)
Are there mandatory obligations on the steps an organization is required to take in the event of a data breach / incident?	The APPI does not provide clear guidance on the steps a data handler must take in case of a data incident other than the incident reporting/notification requirements as stated above (e.g. deadlines of reporting/notification). For completeness, the authority and contact point to which an incident report should be addressed may vary depending on the type of impacted/likely impacted data and the type or nature of the data handler's business (e.g. financial, telecommunications business sectors; APPI, Articles 150, 152). Generally, however, incident reports should be addressed to the PPC (APPI, Article 26) and the data handler must submit its report via the PPC's website.
Are there mandatory obligations to notify a regulator or data subjects about a personal data security breach?	Yes. A report to the appropriate authority (e.g. PPC) and a notification to affected/potentially affected individuals are mandatory in case of an incident in which there is a high possibility of harming an individual's rights and interests. Any data handler involved in a data incident has a reporting obligation in general, but in the case where there was an entrustment of the handling of personal data, if the entrustee reported the incident to the entrustor as soon as possible, the reporting obligation of the entrustee to the authority and affected/potentially affected individuals may be waived.

If "Yes", for regulator notifications and data subject notifications respectively:

(a) When is a notification obligation triggered:

□ Quantitative threshold (e.g. volume of data or number of data subjects involved) – [set out the threshold]

□ Qualitative threshold (e.g. sensitivity of data or risk posed to data subjects) – [set out the threshold]

The reporting obligation to the authority and the notification obligation to affected or potentially affected data subjects are triggered (the triggers for the two are substantially the same), when the incident actually or potentially:

- impacts sensitive personal data;
- results in a risk of property damage,
- was caused by an intentional violation of the law such as unauthorized access; or
- affects at least 1,000 data subjects generally (in specific cases e.g. MyNumber is impacted, 100 data subjects),
- in which case the data handler must notify the impacted/likely impacted data subjects.

(b) What is the timing requirements for making a notification?

- The report to a relevant authority:
    - The initial report: as soon as possible (which is generally interpreted as required within 3-5 days by the Guidelines) after Leakage or its equivalent is detected
    - The final report: 30 days after Leakage or its equivalent is detected in general; 60 days after Leakage or its equivalent is detected in case of intentional breach.

- The notification to relevant individuals:
    - The data handler must promptly notify the individuals concerned when it becomes aware of a reportable incident. "Promptly" means as soon as possible but the specific timing of notification should be determined on a

case-by-case basis.

(c) What content must the notification contain?

- The report to a relevant authority must contain the following information, for example:
  - an overview of the incident;
  - affected or possibly affected data types;
  - number of affected or possibly affected individuals;
  - causes of the incidents;
  - whether there is any secondary damage or risk thereof, and details thereof;
  - how to inform affected/potentially affected data subjects;
  - whether the incident was publicized or not;
  - new security measure to prevent reoccurrence; and
  - any other references.

Please note that a data handler must use the form designated by the relevant authority for such report.

- The notification to relevant individuals must contain the following information.
  - an overview of the incident;
  - affected or possibly affected data types;
  - causes of the incident;
  - whether there is any secondary damage or risk thereof, and details thereof; and
  - any other information useful for the data subject.

DP authority and enforcement focus penalties under DP laws

Who is the main data privacy	The Personal Information Protection Commission Japan ("**PPC**").

authority or regulator in your jurisdiction?

What are the penalties for non-compliance with local data protection laws?

When a data handler does not follow the APPI and other guidelines, the PPC may issue administrative actions such as Collection of Reports and Onsite Inspections of such data handlers, or provide Guidance and Advice to such data handlers, or issue Recommendations and Orders (APPI, Articles 146 - 148).

An administrative penalty of up to JPY 100,000 for a natural person may be imposed in the case of minor breaches such as false response to confirmation requests from data recipients under the APPI in case of data transfers (APPI, Article 185)

Criminal fines and imprisonment may be imposed (APPI, Articles 176 - 184). For example:

- a person that fails to comply with the PPC's Order within Japan may be subject to up to one year of imprisonment or a fine of up to JPY 1 million (APPI, Article 178).
- if a data handler, its employee, its predecessor business or its former employee has provided or misappropriated personal information handled in the course of its business for seeking its own or a third party's illegal profits, such person may be subject to up to one year of imprisonment or a fine of up to JPY 500,000 (APPI, Article 179).
- a person that fails to comply with the PPC's Report or Onsite Inspection as described above or reports fraudulently in response to the PPC's Report may be subject to a fine of up to JPY 0.5 million (APPI, Article 182).

Furthermore, in case of a legal entity, an individual (i.e. representative, agent, employee or other worker) may be subject to the foregoing penalty, and the legal entity itself can be fined up to JPY 100 million (APPI, Article 184).

(a) Do data subjects have any private remedies?

Not under the APPI.

Generally, individuals seek relief from the data handlers through litigation based on tort or beach of contractual obligations.

Has the data privacy regulator issued any notable enforcement guidance or judgments in the last 12-24 months?	In March 2024, the PPC announced Recommendations to a social media company, LY Corporation, based on a data incident involving potential leakage personal data of 302,980 data subjects. In its FY 2024 annual report (available only in Japanese), PPC highlights the following points: ◦ Some violations of the APPI with specific company names, ◦ The PPC's exercise of supervisory authority over private sectors under the APPI in 2024 (and the number of cases in 2023 in parentheses for comparison): Collection of Reports: 67 (73) cases, Guidance and Advice: 395 (333) cases, Recommendations: 1 (3) case, ◦ Incident reports: 14198 (7075) cases, For the year 2024, the number of individuals affected or potentially affected by data incidents per case was most frequently 1,000 or fewer (88.3%), while cases involving more than 50,000 individuals accounted for 0.8%.

Associated Contacts

Charmian Aw

Email Me

Hiroto Imai

Email Me

Maria Yaka

Email Me

Mizue Kakiuchi

Email Me

Singapore

Last updated 16 September 2025

Overview of Personal Data Protection Laws

What is the principal legislation, law or regulation governing personal data protection?	Personal Data Protection Act (PDPA), which was passed in 2012, came into full force in 2014, and was amended in 2020.
Do the jurisdiction's data protection laws have extra-territorial scope?	No. The PDPA only applies to any collection, use or disclosure in Singapore. However, foreign organisations with no physical or legal presence in Singapore could still be subject to the PDPA's obligations so long as it processes personal data within Singapore.

Key definitions under data privacy laws

What are the definitions of: (a) personal data, and (b) sensitive personal data under data protection laws?	**a. Provide examples to distinguish between "personal data" and "sensitive personal data."** (a) Personal data is defined as data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access. (b) Sensitive personal data is not explicitly defined in the PDPA. However, the Personal Data Protection Commission (PDPC)'s Advisory Guidelines on the PDPA for Selected Topics refers to minors' persona data as "generally considered to be sensitive personal data and must be accorded a higher standard of protection under the PDPA". Further, there is a prescribed list of data in the Personal Data Protection (Notification of Data Breaches) Regulations 2021 which if affected in a data breach, is deemed to result in significant harm to an individual, and triggers mandatory data breach reporting to the PDPC, and potentially the affected individual(s) too unless an exemption applies.
What (if any) exceptions apply to the above	

definitions of personal data or sensitive personal data?	An individual's business contact information is excluded from the main data protection obligations in the PDPA. Business contact information is defined as an individual's name, position name or title, business telephone number, business address, business e-mail address, or business fax number and any other similar information about the individual, not provided by the individual solely for his or her personal purposes. However, the Do Not Call Registry obligations in the PDPA continue to apply to business contact information.

Controller vs Processor

Do the jurisdiction's data protection laws include the concept of: (a) a "controller", and (b) a "processor"? How are they defined?	Yes. An organisation that collects, uses or discloses personal data under the PDPA is by default subject to it as a controller. An "organisation" is defined to include any individual, company, association or body of persons, corporate or unincorporated, whether or not (i) formed or recognised under the law of Singapore; or (ii) resident, or having an office or a place of business, in Singapore. This is unless that organisation also falls within the definition of a "data intermediary", which refers to an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation. Data intermediary is therefore synonymous with a "processor" under the PDPA.
Do controllers have any legal obligations to control how processors manage the personal data that the controllers provide to them?	Yes. A controller organisation is responsible for complying with and subject to the same obligations in the PDPA for personal data processed on its behalf and for its purposes by a data intermediary (or processor), as if the personal data were processed by the controller organisation itself.

Legal basis for collection and processing

What are the legal bases permitting an organization to collect and process personal data?	**Consent:** (a) What are the conditions or requirements for obtaining valid consent? Firstly, the individual must have been informed of the purposes for the processing of his/her personal data on or before collecting that data. Secondly, the consent must not be as a condition of providing a product

or service, beyond what is reasonable to provide that product or service. Thirdly, consent must not have been obtained using any deceptive or misleading practices.

(b) Does the jurisdiction's data protection law recognise different types of consent?

Yes. There are two ways for consent to be "deemed" for a particular purpose. Firstly, if an individual voluntarily provided his/her personal data to the organisation for that purpose and it is reasonable that the individual would voluntarily provide the data. Secondly, if the organisation conducts an assessment to determine that the proposed processing of personal data is unlikely to have an adverse effect on the individual; takes reasonable steps to bring to the attention of the individual its intention to process the personal data, the purpose(s) of processing, and a reasonable period within which the individual may object to the processing, and no objection is made.

(c) Can consent be withdrawn?

Yes.

□ "Legitimate interests":

a. What interests are considered legitimate interests?

This is not specifically defined in the PDPA, so a plain literal meaning should be applied.

b. For an organisation to rely on "legitimate interests", what are the relevant requirements or conditions?

Firstly, the processing must be in the legitimate interests of the processing organisation or another person. Secondly, the organisation must conduct an assessment to determine that such legitimate interests outweigh any adverse effect on the individual. Thirdly, the organisation must identify and implement reasonable measures to mitigate such adverse effect on the individual.

□ "Contractual necessity":

a. What purposes would fall under this legal basis?

Any processing (collection, use or disclosure) of an individual's personal data, for the conclusion of performance of a contract, subject to the conditions in the sub-paragraph (b) which immediately follows.

b. For an organisation to rely on this legal basis, what are the relevant requirements or conditions?

The individual provides his/her personal data to an organisation: (i) with a view to entering into a contract with that organisation; or (ii) for the conclusion or performance of a contract between that organisation and another person which is entered into at the individual's request, or which a reasonable person would consider to be in the individual's interest.

□ "Compliance with legal / regulatory requirement".

a. What purposes would fall under this legal basis?

Any processing (including collection, use or disclosure) of personal data where required by any law, including legal privileged, except that the performance of a contract is not an excuse for contravening the PDPA.

b. For an organisation to rely on this legal basis, what are the relevant requirements or conditions?

The processing must be necessary to comply with a legal or regulatory requirement imposed by law.

□ Other legal basis apart from the above:

a. What are the other legal bases?

(i) Business improvement, where processing is done within a group of related corporations to improve or enhance any goods or services provided, to develop new ones, or to learn about and understand the behaviour and preferences of an individual in relation to goods or services provided by the organisation (ii) Research (iii) Business asset transaction (iv) Vital interests of individuals (v) The personal data is publicly available (vi) Processing in the national interest (vii) An artistic, literary, archival or historical purpose (viii) The personal data is processed by a news organisation solely for its news activity (ix) The

processing is necessary for evaluative purposes.

b. What purposes would fall under each legal basis mentioned above in 5.a?

(i) Collecting, using and disclosing of personal data within a group of related corporations. (ii) Use and disclosure of personal data for a research purpose (including historical or statistical research). (iii) The processing is for a business asset transaction that is being contemplated or entered into, where business asset transaction refers to a purchase, sale, lease, merger, amalgamation or any other acquisition, disposal or financing of an organisation or portion of an organisation; an interest in an organisation; or any of the business or assets of an organisation. (iv) and (v) Any purpose so long as the conditions are met (see (c) below). (vi) The processing of personal data is in the national interest. (vii) The processing is for artistic or literary purposes. (viii) The processing is for a news activity. (ix) The processing is for evaluative purposes, which includes determining the eligibility for employment, a promotion, for termination, admission into an educational institution, the award of a contract or other benefits, for selection for an athletic or artistic purpose, the grant of financial assistance, or for insurance.

c. For an organisation to rely on each legal basis mentioned above in 5.a, what are the relevant requirements or conditions?

(i) Firstly, the individual must be either an existing customer or prospective customer of the organisation. Secondly, the purpose for processing the personal data cannot reasonably be achieved without it being in an individually identifiable form. Thirdly, a reasonable person would consider the processing to be appropriate in the circumstances. Fourthly, the related organisations in the group are bound by an agreement requiring the recipient to implement appropriate safeguards for the personal data. (ii) historical and statistical research, subject to the following conditions: a) The research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form; b) There is a clear public benefit to using the personal data for the research purpose; c) The results of the research will not be used to make any decision that affects the individual; and d) In the event the results of the research are published, the organisation must publish the results in the form that does not identify the individual. (vii) The processing is solely for artistic or literary purposes, solely for archival or

	historical purposes, if a reasonable person would not consider the personal data to be too sensitive to the individual to be processed at the proposed time.
If local law recognizes the concept of "sensitive" personal data, are there special rules to the legal bases mentioned in Q.1, or different legal bases than the above, for an organization to collect or process sensitive personal data?	Not Applicable

Transparency / disclosure requirements

Are there any transparency or disclosure requirements under the jurisdiction's data protection laws, requiring disclosure of certain information to data subjects? If yes – What are the items of information that must be disclosed to data subjects?	The organisation's Data Protection Officer's business contact information, and the organisation's data protection policies and complaints process upon request from the data subject.
Are organizations required to have a privacy policy? If yes, must the privacy policy cover the information as in the 'Overview of Personal Data Protection Laws' above, or is any	Yes, and yes. The policy should also include the organisation's data protection officer's business contact information, such as an email address that he/she monitors for data protection related queries.

additional information required to be covered?	

Data of children or minors

Are there specific laws, regulations, rules or guidelines that govern the collection or processing of children's personal data?	Yes, there are advisory guidelines, which are not legally binding, but provide guidance on how the PDPA will be interpreted, applied and enforced with regards to the processing of children's personal data.
What mandatory requirements do those laws, regulations, rules or guidelines provide for the collection or processing of children's personal data?	**a. If consent applies in respect of collecting or processing children's personal data, what constitutes valid consent?** As a rule of thumb, for any individual that is under the age of 13, his/her parental or legal guardian's consent would be required before an organisation can process his/her personal data. The organisation must also have reason to believe that a data subject that is older than 13 does not lack the mental capacity to be able to understand the nature and consequences of giving consent for the processing of his/her personal data. Otherwise, such parental or guardian consent is required.

Direct and e-marketing online tracking and cookies requirements

What constitutes direct marketing under the jurisdiction's data protection laws?	Direct marketing is not specifically defined, but would refer to any marketing that is sent to a person using his/her contact details such as a telephone number, email address, or postal address.
What are the requirements for the use of personal data for direct marketing or e-marketing?	◦ **Consent. What are the consent requirements specific to direct marketing or e-marketing?** Generally, consent is required for direct marketing including e-marketing to individuals. There are additional Spam Control Act rules if the direct marketing is unsolicited and done in bulk. Further, there are exclusions for e-marketing to business representatives in a B2B context. Please also see our comments

under the "Other requirements" checkbox below, in respect of the Do Not Call provisions in Singapore.

- **Disclosure. What are the requirements for disclosing information to data subjects which are specific to direct marketing or e-marketing?**

As nothing additional is specifically prescribed, the usual notification obligations would apply, so data subjects need to be informed of the purposes of processing their personal data, such as the types of marketing that they will be receiving unless they have opted out.

- **Other requirements. What are the other requirements specific to direct marketing or e-marketing?**

Singapore has a national Do Not Call Registry (https://www.dnc.gov.sg/) that enables individuals to subscribe their Singapore telephone numbers so as not to receive phone calls, text and/or fax messages (these are modular options that individuals can select). If a number is subscribed to any of these three DNC registers, an organisation must not send telemarketing via the relevant channel(s) unless it has obtained the clear and unambiguous consent of the individual recipient to do so.

What specific laws, regulations or guidelines (if any) govern the use of cookies and similar online tracking tools?	Not Applicable
What do those laws or guidelines require for the use of cookies or similar online tracking tools?	Not Applicable

Data sharing and engaging processors

Are there any requirements for sharing personal data or engaging third party data processors to process personal data?	If personal data is shared with a third party data processor (or data intermediary in the PDPA), for such processor to process it on the organisation's behalf and pursuant to a written contract, then the controller organisation has the same obligations in the PDPA in respect of such personal data, as if the personal data was processed by it.

Data localization and cross-border transfer

Are there data localization or similar laws that require personal data to be retained in the local jurisdiction?	No.
What are legal mechanisms for cross-border data transfers ?	☐ Data subject consent ☐ Transfers to jurisdictions which are whitelisted or subject to an adequacy decision ☐ Standard data protection clauses (SCCs) ☐ Binding corporate rules (BCRs) ☐ Codes of conduct ☐ Certification mechanisms ☐ Ad hoc contractual clauses ☐ Approval from or registration or filing with local authorities **a. For each of the applicable mechanisms, what are the requirements for the organisation seeking to transfer personal data to rely on such mechanism?** For data subject consent, this needs to be accompanied by a written summary as to how the recipient jurisdiction's personal data protection laws are comparable to the PDPA. **b. What if any derogations are permitted by law?** Derogations not already identified above include: (i) where the personal data is publicly available; and (ii) where the personal data is data in transit, which means personal data transferred through Singapore in the course of onward transportation to a territory outside Singapore,

without the personal data being accessed or used by, or disclosed to, any organisation (other than the transferring organisation or an employee acting for the transferring organisation in the course of employment) while the personal data is in Singapore, except for the purpose of such transportation.

Data subject rights

What are the data subject rights provided under the jurisdictions' data protection law?

□ Right to be informed. What does this right require the organization to do?
The organisation has to provide notification to individuals about the ways in which their personal data is processed, and make available the business contact details of its data protection officer.

□ Right of access. What does this right require the organization to do?
To provide a requesting individual with personal data about him/her that is in its possession or under its control, and information about the ways in which the personal data has been used or disclosed by the organisation within a year before the date of the request. There are specified exceptions to this right in the PDPA.

□ Right to rectification. What does this right require the organization to do?
To correct an error or omission in the personal data about the requesting individual that is in the possession or under the control of the organisation, unless it is satisfied on reasonable grounds that a correction should not be made. There are specified conditions to this exception in the PDPA.

Data protection impact assessments

In what circumstances are data protection impact assessments required?

Data protection impact assessments are not statutorily mandated in Singapore.

Data Protection Officer

Is there a requirement to

Yes.

appoint a DPO? If yes:	
In what circumstances is it required to appoint a DPO?	All cases where there is processing of personal data in Singapore.
Does the DPO have to possess certain qualifications or meet specific requirements? If so, what are these qualifications or requirements?	Not applicable. It is not mandatory but generally recommended that the DPO be contactable during Singapore office hours, and that their business contact details be made available to the public (e.g. on a website privacy policy).
What are the responsibilities of a DPO?	To oversee and ensure the organisation's compliance with the PDPA.

Registration notification or filing requirements

Are there obligations to register with or notify the data protection authority in order to collect or process personal data generally?	Not applicable

Security requirements and breach notification

What obligations does the jurisdiction's data protection law impose, with respect to maintaining security controls to protect personal data from unauthorized access?	Section 24 of the PDPA requires an organisation to make reasonable security arrangements to prevent the unauthorised access, use, disclosure, modification and other similar risks to the personal data in its possession or control.

How is a "data breach" or "data incident" defined?	It refers to the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.
Are there mandatory obligations on the steps an organization is required to take in the event of a data breach / incident?	There are mandatory reporting requirements in cases which trigger such notifications – see our response to sub-question 4 below.
Are there mandatory obligations to notify a regulator or data subjects about a personal data security breach?	**a. When is a notification obligation triggered:** □ Quantitative threshold (e.g. volume of data or number of data subjects involved) – 500 or more. □ Qualitative threshold (e.g. sensitivity of data or risk posed to data subjects) – Likely to cause significant harm to an affected individual. **b. What is the timing requirements for making a notification?** Without undue delay, and no later than 3 calendar days from discovering a notifiable breach. There is an assessment period of up to 30 days for an organisation to determine if a breach is notifiable. **c. What content must the notification contain?** There is a standard form on the Commission's website.

DP authority and enforcement focus penalties under DP laws

Who is the main data privacy authority or regulator in your jurisdiction?	The Personal Data Protection Commission of Singapore, or Infocomm Media Development Authority of Singapore.
What are the	**Do data subjects have any private remedies?**

penalties for non-compliance with local data protection laws?	Yes. Aggrieved individuals can bring a private action under the PDPA before the Singapore courts.
Has the data privacy regulator issued any notable enforcement guidance or judgments in the last 12-24 months?	Yes. All of the enforcement decisions are published on the Commission's website.

Associated Contacts

Charmian Aw

Email Me

Ciara O'Leary

Email Me

Vietnam

Last updated 16 September 2025

Overview of Personal Data Protection Laws

What is the principal legislation, law or regulation governing personal data protection?	The principal legislation governing personal data protection in Vietnam is currently Decree No. 13/2023/ND-CP on Personal Data Protection (**Decree 13**). The adoption of this Decree, which came into effect on 1 July 2023, represented a milestone as the nation's first comprehensive legal document dedicated to data privacy. Vietnam's personal data protection regulatory framework is set to evolve further with the enactment of the Law on Personal Data Protection (**PDPL**) on 1 January 2026. The PDPL will function as the

main data protection law, replacing Decree 13 as the central legal instrument and unifying the fragmented legal landscape.

In addition, the Law on Data, Decree 165/2025/ND-CP with guidance on that law, and Decision 20/2025/QD-TTg, listing critical and core data categories and include provisions applicable to businesses which collect basic data of at least 1 million Vietnamese citizens, sensitive data of at least 100,000 Vietnamese citizens or data on bank accounts, payment history and debt obligations of at least 100,000 Vietnamese enterprises. The Law on Data and its regulations create significant new compliance obligations for any entity involved in large-scale data-related activities in Vietnam and entered into effect on 1 July 2025.

Do the jurisdiction's data protection laws have extra-territorial scope?

Yes. Decree 13 applies to both Vietnam-based and foreign individuals and organisations that are directly or indirectly involved in data processing activities in Vietnam. The PDPL reinforces this principle by stating that it applies not only to Vietnamese organisations but also to any foreign entity processing the data of Vietnamese citizens.

This broad application is a core principle of Vietnam's data protection framework, asserting the state's sovereign control over the personal data of its citizens, regardless of where the processing entity is located.

Key definitions under data privacy laws

What are the definitions of: (a) personal data, and (b) sensitive personal data under data protection laws?

a. Provide examples to distinguish between "personal data" and "sensitive personal data."

Under both Decree 13 and the new PDPL, personal data is defined as any information that identifies or helps identify a specific individual. The PDPL expands this definition to include data in both digital and "other forms," such as traditional paper-based records. Under the PDPL anonymised data falls outside the scope of personal data, but encrypted data is still considered personal data and is therefore subject to the law's requirements.

The Vietnamese framework operates on a two-tiered classification system of "*basic personal data*" and "*sensitive personal data*". Decree 13 provides a non-exhaustive list of examples for both categories. The PDPL defers the detailed enumeration of data types within these categories to be determined by a future government decree, which may provide more flexibility.

(a) **Basic personal data**: Decree 13 defines personal data as

	information about an individual that is either (i) associated with a specific person or (ii) derived from personal activities and helps identify a specific individual when combined with other data and information. The PDPL is expected to broaden this definition to include data about an individual that can be used to identify them either directly or indirectly, covering data in both digital and non-digital forms. (b) **Sensitive personal data**: Both Decree 13 and the PDPL recognise a category of sensitive personal data that is afforded a higher level of protection. Under the PDPL, the list of sensitive personal data will be issued by the Government.
What (if any) exceptions apply to the above definitions of personal data or sensitive personal data?	Under Decree 13, there are no express exceptions to the definitions of personal data or sensitive personal data. Although not expressly stated, Decree 13 should not apply to data that has been anonymised or de-identified, since it can no longer identify a specific individual. The PDPL clarifies that personal data, once anonymised, is no longer considered personal data. Anonymisation is defined as the process of altering or deleting information to create new data that cannot identify or help identify a specific individual.

Controller vs Processor

Do the jurisdiction's data protection laws include the concept of: (a) a "controller", and (b) a "processor"? How are they defined?	Yes, Decree 13 and the PDPL introduce and define four types of parties involved in data processing: (1) a "*data controller*" is an organisation or individual that determines the purpose and means of processing personal data; (2) a "*data processor*" is an organisation or individual that processes personal data on behalf of a controller under a formal contract or agreement; (3) a "*data controller and processor*" is a party that both determines the purpose and directly processes the data; and (4) a "*third party*" is any organisation or individual other than the data subject, controller, or processor that is authorised to process personal data.
Do controllers have any legal obligations to control how processors manage the personal data that the controllers	Yes. The controller shall bear the ultimate responsibility to the data subject for any damages caused by the processing of data, including by its processors. The relationship must be governed by a written contract that specifies the scope and requirements of the processing.

provide to them?

Legal basis for collection and processing

What are the legal bases permitting an organization to collect and process personal data?

□ Consent:

(a) What are the conditions or requirements for obtaining valid consent?

Consent is the primary legal basis for processing personal data in Vietnam. To be considered valid, consent must be a clear, voluntary, and affirmative expression from the data subject, which must be in a format that can be printed and reproduced in writing, including electronic or other verifiable forms. This includes a requirement for "granular consent," where a separate, purpose-specific approval is obtained for each distinct processing activity. The data subject must be fully informed of the type of data to be processed, the purpose, the entities involved, their rights, possible undesirable damages and consequences, and start and end time of processing. Silence or a lack of response does not qualify as consent.

(b) Does the jurisdiction's data protection law recognise different types of consent?

Both Decree 13 and the PDPL recognise express consent, with the requirements outlined in our response in paragraph (a) above.

(c) Can consent be withdrawn?

Yes. While the Decree 13 stipulated a very strict 72-hour deadline for organisations to comply with a withdrawal request, the new PDPL no longer imposes this stringent timeframe. However, upcoming government guidance may introduce additional requirements.

□ "Legitimate interests":

a. **What interests are considered legitimate interests?**
   Decree 13 has no provision on "*legitimate interests*" as the basis for processing personal data without consent. The PDPL recognizes the protection of "*legitimate rights or interests*" of the data subject, other persons, the State, government agencies or organisations as one of the cases of exemption from the consent requirement. However, there is still no detailed guidance on how such "*legitimate rights or interests*" are defined.

b. **For an organisation to rely on "legitimate interests", what are the relevant requirements or conditions?**
Upon the entry into effect of the PDPL on 1 January 2026, in principle it will be possible to invoke the protection of "legitimate rights or interests" to process personal data without consent. However, no detailed guidance is currently available.

□ "Contractual necessity":

a. **What purposes would fall under this legal basis?**
Any data processing to fulfil contractual obligations of the data subject with relevant agencies, organisation, or individuals in accordance with the law. Notably, this legal basis is recognised as one of the cases in which data processing can occur without the express consent of the data subject.

b. **For an organisation to rely on this legal basis, what are the relevant requirements or conditions?**
Organisations shall be permitted to process personal data to the extent necessary to uphold and execute the terms and responsibilities outlined in the relevant contracts or agreements. The PDPL mandates monitoring mechanism when processing personal data without the consent of the personal data subject.

□ "Compliance with legal / regulatory requirement":

a. **What purposes would fall under this legal basis?**
Decree 13 allows disclosure of personal data in accordance with the law. The PDPL contains a broader exception to the consent requirement in "*other cases specified by the law*".

b. **For an organisation to rely on this legal basis, what are the relevant requirements or conditions?**
Processing without consent must be expressly permitted by relevant legislation. The PDPL requires that the processing organisation must have a mechanism to monitor the processing of personal data without data subjects' consent, conduct regular risk and data privacy compliance assessments, take adequate measures to protect personal data, and have a mechanism to deal with complaints.

□ Other legal basis apart from the above:

a. **What are the other legal bases?**
Vietnam allows data processing without obtaining prior data subjects' consent in certain circumstances, including: (i) disclosure in accordance with the law (for example, pursuant to Decree 13); (ii) if necessary for the operations of State authorities as prescribed by

relevant law; (iii) for purposes of national defence, security, social order and safety, major disasters, or dangerous epidemic; (iv) to protect the life, health, interests of the data subject or others in an emergency situation; or (v) as otherwise expressly allowed by law or regulation.

b. **What purposes would fall under each legal basis mentioned above in 5.a?**
Please see our response to sub-question a.

c. **For an organisation to rely on each legal basis mentioned above in 5.a, what are the relevant requirements or conditions?**
For the purpose of protecting the life, health, interests of the data subject or others in an emergency situation, processing parties shall bear the burden of proof. For other cases, it is advisable to maintain written record and evidence.

While Decree 13 does not mandate other requirements and conditions, the PDPL mandates specific monitoring mechanism when processing personal data without the consent of the personal data subject.

If local law recognizes the concept of "sensitive" personal data, are there special rules to the legal bases mentioned in Q.1, or different legal bases than the above, for an organization to collect or process sensitive personal data?

Yes.

a. **What are the special rules / different legal bases?**
The processing of sensitive personal data requires (i) express and separate consent from the data subject, as well as (ii) special protection measures.

b. **For an organisation to rely on each legal basis mentioned above in 6.a, what are the relevant requirements or conditions?**
Decree 13 currently mandates the following requirements for processing sensitive personal data:

i. **Express notification requirement**: When processing sensitive personal data, the data subject must be expressly notified that the data requiring processing is sensitive personal data. This is an additional notification requirement beyond the general obligation to inform data subjects about personal data processing activities.
ii. **Enhanced protection measures**: Organisations processing sensitive personal data must adopt all general and standard personal data protection measures, and supplement them with specific measures tailored to sensitive data.
iii. **Appointment of dedicated personnel/department**: Organisations that process sensitive personal data are required to appoint a department with the function of protecting personal data and a dedicated person in charge of personal data protection, whose information must be provided to the

Ministry of Public Security (**MPS**) in its role as regulator tasked with authority to implement personal data protection laws and regulations. While the PDPL does not contain the same level of details, the upcoming government guidance may elaborate on the specific requirements.

Transparency / disclosure requirements

Are there any transparency or disclosure requirements under the jurisdiction's data protection laws, requiring disclosure of certain information to data subjects? If yes – What are the items of information that must be disclosed to data subjects?	Under Decree 13, prior to data processing, organisations must disclose the purpose of processing, type of data being processed, method of processing personal data, information on the relevant parties involved in the processing purposes, possible undesirable damages and consequences, start and end time of the data processing, and the data subject's rights. The PDPL maintains the above requirements, and introduces specific obligations for industries, such as banking and finance, or special types of data, such as localization or biometric data, requiring data controllers and processors to notify data subjects of any damage, leakage or loss.
Are organizations required to have a privacy policy? If yes, must the privacy policy cover the information as in the 'Overview of Personal Data Protection Laws' above, or is any additional information required to be covered?	Yes, and yes. While Decree 13 and the PDPL do not explicitly mandate a "privacy policy," it requires organisations to document their processing activities and obtain prior consent from data subjects, which in practice necessitates an accessible and reproducible privacy policy or statement.

Data of children or minors

Are there specific laws, regulations, rules or guidelines that govern the collection or	Vietnam has specific, legally binding requirements for the collection and processing of children's personal data. The Vietnamese law classifies children as those under the age of 16.

processing of children's personal data?

What mandatory requirements do those laws, regulations, rules or guidelines provide for the collection or processing of children's personal data?

a. **If consent applies in respect of collecting or processing children's personal data, what constitutes valid consent?**

Decree 13 provides for a tiered consent model for children.

(i) For children under the age of 7, consent for data processing must be given by their parent or legal guardian.

(ii) For children aged 7 to under 16, a dual consent model applies, requiring consent from both the child and their parent or legal guardian, unless a non-consent legal basis is applicable.

The PDPL partially abolished the above dual consent requirement. The parent's or guardian's consent is sufficient in most cases of processing of personal data of children. The requirement for dual consent is maintained only for the processing of personal data of children aged from 7 to 16 years old with the aim of publishing or disclosing information about their private life and personal secrets.

Direct and e-marketing online tracking and cookies requirements

What constitutes direct marketing under the jurisdiction's data protection laws?

While not expressly defined, direct marketing is comprehensively regulated under the umbrella of "*advertising by messages, emails, and calls*" and the processing of personal data for "*advertising and marketing purposes*".

What are the requirements for the use of personal data for direct marketing or e-marketing?

- **Consent. What are the consent requirements specific to direct marketing or e-marketing?**

Yes, express consent is required for direct marketing. The consent must be specific to the marketing purpose (e.g., the content, method, form, and frequency of the product introduction) and must include an opt-out mechanism.

- **Disclosure. What are the requirements for disclosing information to data subjects which are specific to direct marketing or e-marketing?**

Yes. Consent for direct marketing or e-marketing is generally similar to normal personal data processing, and should be covered under the initial data processing notice. In addition, advertising messages or emails must be properly labelled with either "[AD]" or "[QC]" at the beginning. Advertising emails must also include information about the advertiser, such as name, phone number, email address, geographical address, and website/social network (if any).

- **Other requirements. What are the other requirements specific to direct marketing or e-marketing?**

Yes, Decree 91/2020/ND-CP on anti-spam calls, messages and emails mandates additional requirements.

i. **Do-Not-Call Register compliance**: Advertisers are prohibited from sending advertising messages or making advertising calls to phone numbers listed in the "Do-Not-Call Register," a list maintained for users who have registered not to receive such communications.
ii. **Clear opt-out mechanism**: There must be reasonable solutions and convenient conditions for users to refuse to or unsubscribe from receiving advertising messages or emails. Upon receiving an opt-out request, the advertiser must promptly stop sending the refused communications and send a confirmation.
iii. **Frequency limitations**: Unless otherwise agreed by the user, an advertiser may send up to three advertising messages, up to three advertising emails, and make one advertising call to a specific phone number or email address within a 24-hour period.
iv. **Record-keeping**: Advertisers are required to retain records of consent, refusal, and opt-out requests and confirmations for a minimum of one year to facilitate inspection and supervision.

What specific laws, regulations or guidelines (if any) govern the use of cookies and similar online tracking tools?

Vietnam does not have a specific law dedicated to cookies. However, under Decree 13, cookies are considered a form of personal data because they reflect a data subject's online activity history. The new PDPL provides more direct regulations, requiring social media platforms and Over-the-Top (OTT) services to offer a "Do Not Track" feature, allowing users to decline cookie tracking and data sharing. The law also states that location tracking requires the data subject's consent or a legal order.

What do those laws or guidelines require for the use of cookies or similar online

Any organisation using cookies or similar trackers must inform users and obtain their consent, consistent with the generally applicable consent requirements for personal data processing.

tracking tools?

Data sharing and engaging processors

Are there any requirements for sharing personal data or engaging third party data processors to process personal data?	When a data controller engages a third-party data processor, it remains responsible for the personal data, as if the processing were conducted by the controller itself. This relationship must be governed by a written agreement that defines the responsibilities of each party and specifies the protective measures to be implemented. The risks resulting from sharing personal data or engaging third party data processors must be assessed in the mandatory impact assessment reports and appropriate measures must be taken to mitigate such risks.

Data localization and cross-border transfer

Are there data localization or similar laws that require personal data to be retained in the local jurisdiction?	Yes, entities established in Vietnam are required to maintain personal data in the local jurisdiction. While there is no blanket data localisation requirement applicable to foreign entities, certain sector-specific regulations, such as the Cybersecurity Law, can impose data localisation requirements on specific service providers (e.g., social media, e-commerce and telecom) for certain types of data (including personal data of users in Vietnam) if the foreign entity refused to comply with lawful requests from the authorities to provide information.
What are legal mechanisms for cross-border data transfers ?	☐ Data subject consent ☐ Transfers to jurisdictions which are whitelisted or subject to an adequacy decision ☐ Standard data protection clauses (SCCs) ☐ Binding corporate rules (BCRs) ☐ Codes of conduct ☐ Certification mechanisms ☐ Ad hoc contractual clauses ☐ Approval from or registration or filing with local authorities a. **For each of the applicable mechanisms, what are the requirements for the organisation seeking to transfer personal data to rely on such mechanism?** The primary legal mechanism for cross-border data transfers is the lawful consent from data subjects, and an Offshore Transfer Impact Assessment (**OTIA**) dossier must be prepared and submitted to the MPS within 60 days of the commencement of the transfer and must

be updated in case of (ii) changes from the submitted dossier (under Decree 13) or (ii) every six months for any changes or immediately following critical changes (under the PDPL).

Unlike GDPR, Vietnam does not rely on adequacy decisions, standard contractual clauses (SCCs) in the EU sense, or Binding Corporate Rules (BCRs) as standalone mechanisms for transfer.

b. **What if any derogations are permitted by law?**
While Decree 13 does not provide for any exemption for the OTIA, the PDPL introduces several specific exemptions to this requirement. These include (i) transfers by competent state authorities, (ii) the storage of employee data on cloud services, (iii) cases where the data subject transfers its own data across borders, or (iv) other cases prescribed by the Government.

While these exemptions offer some relief, the overall framework remains centred on proactive, government-led oversight. The MPS has the authority to inspect cross-border transfers and can suspend them if they are found to be non-compliant or if they are deemed to harm national interests.

Data subject rights

What are the data subject rights provided under the jurisdictions' data protection law?

□ Right to be informed. What does this right require the organisation to do?
Yes, this is applicable. Data subjects are entitled to be informed of the processing activities. Organisations must seek express consent of the data subjects prior to data processing and keep them informed of data processing activities.

□ Right of access. What does this right require the organisation to do?
Yes, this is applicable. Data subjects have the right to access and view their personal data, as well as request a copy. Under Decree 13, organisations must provide the data subject with their personal data when requested under a strict 72-hour deadline with specific procedures. While the PDPL no longer mandates the same deadline, further implementing regulations for the PDPL may introduce additional requirements.

□ Right to rectification. What does this right require the organisation to do?
Yes, data subjects have the right to request the correction of inaccurate

personal data. Under Decree 13, organizations must handle the rectification request within a strict 72-hour deadline, but belated response is permissible. While the PDPL no longer mandates the same deadline, further implementing regulations for the PDPL may enact additional requirements.

□ Right to erasure. What does this right require the organisation to do?
Yes, data subjects have the right to request the deletion of their personal data, unless the exceptions apply. Under Decree 13, organisations must handle the erasure request within a strict 72-hour deadline. While the PDPL no longer mandates the same deadline, additional requirements may be enacted.

□ Right to restrict processing. What does this right require the organisation to do?
Yes, data subjects have the right to restrict the processing of their data, unless the law provides otherwise. Under Decree 13, organisations must handle the restriction request within a strict 72-hour deadline. While the PDPL no longer mandates the same deadline, additional requirements may be enacted.

□ Right to data portability. What does this right require the organisation to do?
Yes, data subjects have the right to receive their data in a structured, commonly used format to transfer it to another organisation. Under Decree 13, organisations must handle the request within a strict 72-hour deadline and following a specific procedure. While the PDPL no longer mandates the same deadline, additional requirements may be enacted.

□ Right to object. What does this right require the organisation to do?
Yes, data subjects have the right to object to the processing of their data, unless the law provides otherwise. Under Decree 13, organisations must handle the objection request within a strict 72-hour deadline. While the PDPL no longer mandates the same deadline, additional requirements may be enacted.

□ Rights related to automated decision making including profiling. What does this right require the organisation to do?
Yes, data subjects have the right to be informed about and object to decisions based solely on automated processing.

Data protection impact assessments

In what circumstances are data protection impact assessments required?	Both the Decree 13 and the PDPL require that data controllers and processors prepare and submit a personal data processing impact assessment (**PIA**) dossier to the MPS within 60 days of the commencement of data processing activities. Similar to the OTIA dossier, the PIA dossier must be updated in case of (ii) changes from the submitted dossier (under Decree 13) or (ii) every six months for any changes or immediately following critical changes (under the PDPL).

Data Protection Officer

Is there a requirement to appoint a DPO? If yes:	Yes.
In what circumstances is it required to appoint a DPO?	Vietnamese law requires organisations to appoint a DPO or a dedicated data protection department. While this is a general requirement, the new PDPL provides a five-year grace period for startups and small businesses to comply, unless they are primarily engaged in data processing, directly handle sensitive data, or process a large volume of personal data.
Does the DPO have to possess certain qualifications or meet specific requirements? If so, what are these qualifications or requirements?	While the Decree 13 was vague on DPO qualifications, the PDPL now requires DPOs to be "qualified" in accordance with forthcoming government regulations. The new law also explicitly allows organisations to outsource this function to external qualified data protection service providers.
What are the responsibilities of a DPO?	It is generally understood that the primary responsibility of the DPO is to oversee and ensure the organisation's compliance with all applicable data protection laws. Future government regulation will further elaborate the specific DPO responsibilities.

Registration notification or filing requirements

Are there obligations to register with or	Yes. a. **What are these obligations and their timing requirements?**

notify the data protection authority in order to collect or process personal data generally?

Both Decree 13 and the PDPL impose mandatory filing obligations for specific trigger events, including the mandatory submission of the PIA and OTIA dossiers to the MPS within 60 days of the commencement of the relevant processing or transfer activity.

In addition, please refer to Q14 on notification requirements applicable to data privacy breaches.

b. **Are there exemptions to these obligations of notification or registration?**

The PDPL does provide a five-year grace period for startups and small businesses, exempting them from the PIA and/or OTIA filing requirements unless they are primarily engaged in data processing, directly handle sensitive data, or process a large volume of personal data. There are also exemptions from duplicating OTIA and PIA filings under the Law on Data, if such filings were made under the PDPL.

Please refer to Q9 on the specific exemptions to the OTIA requirement under the PDPL.

Security requirements and breach notification

What obligations does the jurisdiction's data protection law impose, with respect to maintaining security controls to protect personal data from unauthorized access?

Vietnam mandates implementing reasonable and standard security arrangements (including technical and management measures) to protect personal data from unauthorised access, use, disclosure, or other similar risks. The PDPL introduces more specific and detailed security requirements for high-risk data processing activities involving banking and finance personal data, personal localization, biometrics, social media and for emerging technologies like AI and cloud computing.

How is a "data breach" or "data incident" defined?

While Decree 13 does not provide for any specific definition of a data breach, the Law on Cyber Information Security and its guiding regulations do define "*data security breach*" as an information or information system being attacked or harmed which affects the integrity, security or usability of information. Additionally, a data breach also includes any unauthorised processing, disclosure, loss, or destruction of personal data. Please also refer to our response to sub-question 4(a) below for more details on determining a data breach.

Are there mandatory obligations on the steps an organization is required to take in the event of a data breach / incident?	Yes, there are mandatory reporting requirements following trigger events. Please see our response to sub-question 4 below.
Are there mandatory obligations to notify a regulator or data subjects about a personal data security breach?	a. **When is a notification obligation triggered:** □ Quantitative threshold (e.g. volume of data or number of data subjects involved) □ Qualitative threshold (e.g. sensitivity of data or risk posed to data subjects) Under Decree 13, a notification obligation is triggered upon the detection of a breach of regulations on protection of personal data. This includes instances such as discovering breaches of personal data security, personal data being processed for unintended purposes or against the original agreement/law, the data subject's rights not being protected or properly exercised, or other cases as prescribed by law. Under the PDPL, the obligation is triggered upon detection of breaches of personal data protection regulations that may (i) harm national defence, security, social order, and safety or (ii) infringe on the life, health, honour, dignity, and property of personal data subject matters. The PDPL also introduces sector-specific obligations in respect of special types of personal data, such as data used in banking and finance, requiring the relevant organisations to notify data subjects of any damage, leakage or loss. The Government will further elaborate on the notification requirements in a future guiding decree. b. **What is the timing requirements for making a notification?** Formal notification to the MPS (Department of Cybersecurity and Hi-tech Crime Prevention – A05) must be made within 72 hours after the breach occurs. While Decree 13 allows notifications made after the expiry of the 72-hour deadline, the PDPL no longer provides for this exception. Additionally, if a personal data processor detects a breach, it must notify the relevant personal data controller as soon as possible.

c. **What content must the notification contain?**
Under Decree 13, notifications must be submitted using Form No. 03 prescribed with Decree 13 and include the following details:

i. description of the nature of the breach, including: time and place of the violation; specific violation committed; organisation, individual, types of personal data, and the amount of relevant data involved;
ii. contact details of the employee(s) assigned to protect the data or the organisations or individuals responsible for personal data protection;v
iii. description of the consequences and damage that may occur due to the breach; and
iv. description of measures for handling and minimizing the harm caused by the breach.

The notification form also requires general information about the organisation/enterprise, such as its name, address, registration certificate number, phone number, and website.

For the PDPL, the Government will provide the specific notification template in the upcoming guiding decree.

d. **Are there any other requirements for making notifications?**
Yes, the personal data controllers or the personal data controller and processors are required to confirm the breach in writing to the MPS and cooperate with the MPS in handling the breach.

DP authority and enforcement focus penalties under DP laws

Who is the main data privacy authority or regulator in your jurisdiction?	The primary regulatory body is the MPS acting through its specialised agency responsible for personal data protection - the Department of Cyber Security and High-Tech Crime Prevention (**A05**).
What are the penalties for non-compliance with local data protection laws?	Non-compliance with personal data protection regulations may be subject to administrative sanctions, or criminal prosecution, depending on the severity. The PDPL introduces a new and substantially more punitive penalty regime. This represents a fundamental shift from the previous system, which relied on general sanction decrees with comparatively lower fines.

a. **Do data subjects have any private remedies?**

	Yes. Data subjects have the right to claim compensation for damages when a violation of personal data protection regulations occurs, unless otherwise agreed by the parties or provided for by law.
Has the data privacy regulator issued any notable enforcement guidance or judgments in the last 12-24 months?	Given the recent enactment of Decree 13, and the fact that the new PDPL is not yet in force, there have not been any publicly disclosed enforcement judgments or guidance documents issued by the MPS. However, the government has been focusing on raising awareness and encouraging voluntary compliance.

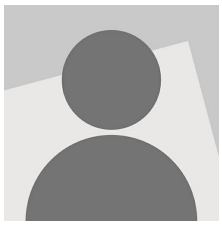
Associated Contacts

Gaston Fernandez

Email Me

Duong Pham

Email Me



Hanh VU

Email Me

Disclaimer