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.

Definitions

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 Bases for 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.

□ 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

Are there any transparency or disclosure requirements	Under APP 5, when an organisation collects personal information, it must take reasonable steps to notify the individual of specific matters. This includes:

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 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).

Minors' Data

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 Marketing, Online Tracking and Cookies

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 Processor Obligations

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.

Cross-Border Transfers

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 Requirements

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

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 and Breach Notification

What obligations does the jurisdiction's data protection law impose, with respect to maintaining security controls	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

to protect personal data from unauthorized access?	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.

Regulatory Authority and Enforcement

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?	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.

Do data subjects have any private remedies?

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

Ciara O'Leary

Singapore
Email Me

Singapore
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.

Definitions

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	None

sensitive personal data?

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 Bases for 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 collect or process sensitive personal data?	Not Applicable

Transparency

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.

Minors' Data

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	Not Applicable

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

Direct Marketing, Online Tracking and Cookies

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 Processor Obligations

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.

Cross-Border Transfers

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 Requirements

Is there a requirement to appoint a DPO? If yes:	No
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?	No
What are the responsibilities of a DPO?	Not Applicable

Registration

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

Security 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.

Regulatory Authority and Enforcement

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.

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

Charmian Aw

Singapore

Email Me

Tommy Liu

Hong Kong

Email Me

Kenneth Cheung

Hong Kong

Email Me

Ciara O'Leary

Singapore

Email Me

India

Last updated 02 November 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 India is the Digital Personal Data Protection Act, 2023 ("**DPDPA**") read with the subordinate rules made thereunder, i.e., the (draft) Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**").

Although the DPDPA was promulgated in 2023 and formally notified into law in the Official Gazette after approval by both houses of Parliament and receiving the President's assent, it has not yet become operational.

Unlike other legislations that become effective upon notification in the Official Gazette, the DPDPA's substantive provisions remain inoperative until an effective date is notified by the Indian Government. It is anticipated that the DPDPA will be brought into effect once the Data Protection Board is established and the Central Government finalizes the DPDP Rules, which will provide interpretative guidance on procedural steps and enforcement methodology. The Minister of Electronics and Information Technology has announced that the DPDP Rules were expected to be finalized by the end of September 2025, which is a deadline that has not been adhered to. We expect that the DPDP Rules will be notified in the upcoming weeks.

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

Yes, if the processing of the personal data is undertaken outside the territory of India but is in connection with any commercial activity (associated with the offering of goods or services to data subjects within India), the DPDPA would apply, even for such extraterritorial personal data processing.

Definitions

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

a. personal data is defined as any data about an individual who is identifiable by or in relation to such data; and
b. sensitive personal data is not defined and there is no distinction between personal data and sensitive personal data under the DPDPA.

protection laws?

What (if any) exceptions apply to the above definitions of personal data or sensitive personal data?	The provisions of the DPDPA do not apply to: a. personal data processed by an individual for any personal or domestic purpose (i.e., not for commercial use); b. personal data that is disclosed publicly, or compelled to be disclosed publicly by: (a) the data subject to whom such personal data relates; or (b) any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available; and c. personal data as physical records, and processed, stored or collected in a non-digitized format without it being digitized (i.e., converted into machine-readable format).

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. A data fiduciary[1] (hereinafter referred to as the "controller" to ensure consistency of reference, since this is a controller-akin definition under DPDPA) means any person who alone or in conjunction with other persons, determines the purpose and means of processing of personal data. b. A data processor[2] (*hereinafter referred to as the processor since this is a term synonymous with the definition of a "processor" under the GDPR*) means any person who processes personal data on behalf of a controller. References 1. Equivalent to a controller under the EU GDPR (Regulation (EU) 2016/679) 2. Akin to a processor under the EU GDPR (Regulation (EU) 2016/679)
Do controllers have any legal obligations to control how processors manage the personal data that the controllers provide to them?	Yes, the controller is required to engage any processor only through a valid contract. Such a contract (which may be referred to by any nomenclature but is akin to a data processing agreement) must include appropriate provisions mandating that the processor implement reasonable security safeguards. The controller is required to ensure compliance with the provisions of the DPDPA and the DPDP Rules in respect of any processing undertaken by it or on its behalf by a contracted processor.

Legal Bases for Processing

What are the legal bases	The DPDPA recognizes lawful purposes for processing of personal data that are: (i) consent; and (ii) legitimate uses.

permitting an organization to collect and process personal data?

The following are identified as legitimate uses under the DPDPA:

a. Processing for the purpose for which the data subject has voluntarily shared their personal data with the controller, and where the data subject has not withdrawn or refused their consent for its use;
b. Processing for the State or its instrumentalities to provide the data subject with any subsidy, benefit, service, certificate, license, or permit, if:
    i. The data subject has earlier consented to the State or its instrumentalities processing their personal data for such purposes; or
    ii. The personal data already exists in digital form, or has been digitized from official records maintained by the State or its instrumentalities and notified by the Central Government.

    Both of the aforesaid processing activities are required to follow the standards set by the Central Government's policy or the Indian data protection laws.
c. Processing for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of security, sovereignty and integrity of India;
d. Processing for meeting any legal obligation that requires any person to share information with the State or its instrumentalities, as long as such disclosure complies with the applicable law;
e. Processing to comply with any judgment, decree, or order, including those related to contractual or civil claims, issued under any applicable law outside India;
f. Processing for responding to a medical emergency involving a threat to the life or immediate threat to the health of the data subject or any other individual;
g. Processing for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health;
h. Processing for taking measures to ensure safety of, or provide assistance or services to, any individual during any disaster, or any breakdown of public order; or
i. Processing for employment purposes or to protect the employer from loss or liability, including preventing corporate espionage, safeguarding trade secrets, intellectual property, and confidential information, or providing any service or benefit requested by an employee.

□ Consent

a. What are the conditions or requirements for obtaining valid consent?
    i. Every request made to a data subject for consent is required to be accompanied or preceded by a notice given by the controller to the data subject, informing them of the particulars listed in point 5.1 (What are the items of information that must be disclosed to data subjects).
    ii. The consent must be: (a) free, (b) specific, (c) informed, (d) unconditional, (e) unambiguous, and (f) with an express, affirmative action (which is not implied), signifying an agreement to the processing of personal data for the specified purpose. The consent obtained for

processing should be limited to personal data as is necessary for the purpose specified.

b. Does the jurisdiction's data protection law recognize different types of consent?
   No, the DPDPA does not recognize different types of consent.
c. Can consent be withdrawn?
   Yes, consent can be withdrawn by a data subject. The controller is required to ensure that the ease of withdrawal of consent should be comparable to the ease with which such consent was given by the data subject.

"Legitimate interests"

No, legitimate interest is not valid grounds for processing of personal data without consent.

"Contractual necessity"

No, contractual necessity is not valid grounds for processing of personal data without consent.

"Compliance with legal/regulatory requirement"

a. What purposes would fall under this legal basis?
   As set out above (in our response to the query for what are the legal bases permitting an organization to collect and process personal data), processing for the following purposes will fall under compliance with legal and regulatory requirement:
   i. Processing for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of security, sovereignty and integrity of India;
   ii. Processing for meeting any legal obligation that requires any person to share information with the State or its instrumentalities, as long as such disclosure complies with the applicable law;
   iii. Processing to comply with any judgment, decree, or order, including those related to contractual or civil claims, issued under any applicable law outside India; and
   iv. Processing for the State or its instrumentalities to provide the data subject with any subsidy, benefit, service, certificate, license, or permit, if:
      1. The data subject has earlier consented to the State or its instrumentalities processing their personal data for such purposes; or
      2. The personal data already exists in digital form, or has been digitized from official records maintained by the State or its instrumentalities and notified by the Central Government.

   Both of the aforesaid processing activities are required to follow the standards set by the Central Government's policy or the Indian data protection laws.
b. For an organization to rely on this legal basis, what are the relevant requirements or conditions?

In the specific instance where a State or its instrumentality is processing personal data for provision or issuance of a subsidy, benefit, service, certificate, license or permit to the data subject, they are required to adhere to the policy issued by the Central Government or any law for the time being in force for the governance of personal data.

Except for the aforementioned obligation cast upon the State and its instrumentalities, there are no specific requirements or conditions for organizations to rely on legitimate uses under the DPDPA, and the exemptions for obtaining consents are applicable to all organizations undertaking processing on the basis of legitimate uses under the DPDPA.

Other legal basis apart from the above

There are no other legal basis (i.e., lawful purpose under the DPDPA) for processing other than: (i) consent; and (ii) legitimate uses, as set out above (What are the legal bases permitting an organization to collect and process personal data?).

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?

The DPDPA does not recognize the concept of "sensitive" personal data; hence, this is not applicable.

Transparency

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

The following particulars must be disclosed to the data subject prior to collecting their personal data:

a. an itemized description of the personal data being collected;
b. the specified purpose of, and an itemized description of the goods or services to be provided or uses to be enabled by, such processing of personal data;
c. the manner and a communication link through which a data subject can: (a) withdraw their consent; (b) exercise their rights under the

data subjects? If yes – what are the items of information that must be disclosed to data subjects?	DPDPA; and (c) make a complaint to the Data Protection Board, which is yet to be constituted under the DPDPA; and d. contact details of a data protection officer (if applicable) or any person who can answer questions on behalf of the controller.
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?	There is no explicit obligation cast on the controller to have a privacy policy under the DPDPA, however, the controller is required to provide a privacy notice to the data subject prior to obtaining their consent. The aforesaid privacy notice should include the information as set out in *(What are the items of information that must be disclosed to data subjects?)* above, such that the data subject can make an informed decision with respect to the processing of their personal data. Additionally, the privacy notice should be understandable independently of any other information provided by the controller. The privacy notice and the request for obtaining consent should be provided in English or any of the 22 languages specified in the Eighth Schedule to the Constitution of India.

Minors' Data

Are there specific laws, regulations, rules or guidelines that govern the collection or processing of children's personal data?	Yes, the DPDPA lays down specific provisions governing the collection and 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?	The following mandatory requirements must be followed by the controllers while processing the personal data of children: a. Implementing appropriate technical and organizational measures to obtain verifiable consent of the parent or the lawful guardian of such child (as the case may be), where the adult identifying as a parent or the lawful guardian of such child is identifiable if required in connection with compliance with any law; b. Not undertaking such processing of personal data that is likely to cause any detrimental effect on the well-being of a child; and c. Not undertaking tracking or behavioral monitoring of children or targeted advertising directed at children.

However, the DPDPA prescribes that if the Central Government is satisfied that a controller processes children's personal data in a verifiably safe manner, it may notify an age limit above which that controller will be exempt from some or all obligations under points (a) and (c) above.

Additionally, the DPDPA and DPDP Rules provide that the processing of personal data of children by the following controllers for the conditions specified herein would be exempt from the requirements listed in points (a) and (c) above:

Clinical/mental health establishment or healthcare professional.	Processing for the provision of healthcare services.
Allied healthcare professionals.	Processing for supporting the implementation of any healthcare treatment.
Educational institution(s).	Processing for educational activities or in the interest of safety of the children enrolled.
Crèche or child day care.	Processing for tracking and behavioral monitoring in the interests of safety of children.
Controller engaged by educational institution or crèche.	Processing for tracking the location during transportation from the institutes.

The DPDPA and the DPDP Rules prescribe that the processing of the personal data of children for the following purposes is exempt from the aforementioned obligations listed in points (a) and (c) of this section, if the processing is undertaken in accordance with the following conditions:

For the exercise of power or discharge of function for safety of child, under applicable law at the time.	Processing to the extent necessary for this purpose.

For providing or issuing of any subsidy, benefit, service, certificate, license or permit under law or public policy.	Processing to the extent necessary for this purpose.
For creating user account for email communication.	Processing to the extent necessary for creating and using the account for communication.
For ensuring information detrimental to children is not available to them.	Processing to the extent necessary for this purpose.
For confirmation by the controller that the data subject is not a child.	Processing to the extent necessary for verification.

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

i. As stated above, to constitute valid consent for the processing of personal data of children, **verifiable** consent of the parents or the lawful guardian (as the case may be) must be obtained.
ii. "Verifiable" consent means undertaking appropriate technical and organizational measures to obtain consent of the parent or the lawful guardian of such child (as the case may be) where the adult identifying as a parent or the lawful guardian of such child is identifiable if required in connection with compliance with any law.

Direct Marketing, Online Tracking and Cookies

What constitutes direct marketing under the jurisdiction's data protection laws?	The DPDPA does not prescribe the meaning of direct marketing.
What are the requirements for the use of personal data for direct marketing or e-marketing?	In accordance with the DPDPA, undertaking tracking or behavioral monitoring of children or targeted advertising directed at children by controllers is not permitted. **□ Consent. What are the consent requirements specific to direct marketing or e-marketing?** The DPDPA does not prescribe a distinct classification for direct marketing or e-marketing; accordingly, there are no specific consent requirements.

□ Disclosure. If applicable, what are the requirements for disclosing information to data subjects which are specific to direct marketing or e-marketing?

No specific requirements.

□ Other requirements. If applicable, what are the other requirements specific to direct marketing or e-marketing?

No specific requirements.

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 governing the use of cookies or similar online tracking tools. However, the provisions of the DPDPA will effectively govern the collection and processing activities in the event that the cookies or similar online tracking tools collect any personal data of a data subject.
What do those laws or guidelines require for the use of cookies or similar online tracking tools?	Not Applicable

Data Sharing and Processor Obligations

Are there any requirements for sharing personal data or engaging third party data processors to process personal data?	The controller is required to engage any processor only through a valid contract and include appropriate provision in the contract for the processor to undertake reasonable security safeguards. Additionally, the controller is required to ensure compliance with the provisions of the DPDPA and the rules made thereunder in respect of any processing undertaken by it or on its behalf by a processor.

Cross-Border Transfers

Are there data localization or similar laws that require personal data to be retained in the local jurisdiction?	a. There data localization requirements under the DPDPA which are only applicable to significant data fiduciaries[1]. A significant data fiduciary must take steps to ensure that specific categories of personal data identified by the Central Government, based on recommendations from a committee, is processed with the restriction that both the personal data and the related traffic data are not transferred outside India. As of the date of this response, such specific categories of personal data have not been identified.

b. The DPDPA also empowers the Central Government to restrict the transfer of personal data to certain country(ies) or territory(ies) outside India by way of a notification. As of the date of this response, no notification to this effect has been promulgated by the Central Government.
c. Transfer of personal data outside India for activities related to offering goods or services to individuals in India is allowed only if the controller follows any requirements the Central Government sets through general or special orders. As of the date of this response, no such orders have been passed by the Central Government.

References

1. Please note that while the DPDPA does not define "sensitive personal data" it empowers the Central Government to designate "significant data fiduciaries" based on factors including the: (i) volume and sensitivity of the personal data, (ii) risk to the rights of a data subject, (iii) potential impact on the sovereignty and integrity of India, (iv) risk to electoral democracy, and (v) security of the State and public order, and imposes additional obligations on entities handling data deemed to carry higher risks. The introduction of such definitions or classes of controllers may cause sub-classes of personal data, which is sensitive, to be categorized.

What are legal mechanisms for cross-border data transfers ?

 Data subject consent.

The controller seeking to transfer personal data should have validly obtained the consent of the data subject for the collection and processing of personal data.

a. For each of the applicable mechanisms, what are the requirements for the organization seeking to transfer personal data to rely on such mechanism?
The controller seeking to transfer personal data should have validly obtained the consent of the data subject for the collection and processing of personal data. There are no other specific requirements for the transfer of personal data under the DPDPA.

   As stated above, transfer of personal data outside India for activities related to offering goods or services to individuals in India is allowed only if the controller follows any requirements the Central Government sets through general or special orders, especially when sharing such data with any foreign State, or with any person, entity, or agency controlled by a foreign State.

b. What if any derogations are permitted by law?
There are no other specific derogations or exceptions specifically contemplated by the DPDPA.

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 controllers are required to provide the following information to the data subject prior to collection of their personal data:

a. Personal data being collected;
b. Purpose for collection of personal data;
c. Rights of the data subjects under the DPDPA;
d. Manner of exercising rights under the DPDPA;
e. Communication link through which the data subjects can make a complaint to the Data Protection Board; and
f. Contact details of a data protection officer (if applicable) or a person who can respond to the data subjects on behalf of the controller.

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

The data subjects can make a request to the controller for accessing their personal data in the manner prescribed by the controller through the communication link provided by the controller on their website or app, or both, and by furnishing the particulars published by the controller for exercising the right of access.

The data subject can make a request to access the following:

a. A summary of personal data which is being processed by the controller and the processing activities undertaken by the controller with respect to such personal data;
b. The identities of all other controllers and processors with whom the personal data has been shared by the controller, along with a description of the personal data shared; and
c. Any other information related to the personal data of such data subject and its processing, as may be requested by the data subject.

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

The data subjects can make a request to the controller for correction, completion, or updating of their personal data in the manner prescribed by the controller through the communication link provided by the controller on their website or app, or both.

As per the request of the data subject, the controller is required to:

a. Correct the inaccurate or misleading personal data;
b. Complete the incomplete personal data; and
c. Update the personal data.

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

The data subjects can make a request to the controller for erasure of their personal data in the manner prescribed by the controller through the communication link provided by the controller on their website or app, or both, and by furnishing the particulars published by the controller for exercising the right of erasure.

The controller is required to erase the personal data unless retention of the personal data is necessary for: (i) the specified purpose for which it was collected; or (ii) compliance with any applicable law. Upon receipt of a request for erasure, the controller is required to cause the processor to erase the personal data made available to the processor by the controller.

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

While there is no specific right to restrict processing of personal data under the DPDPA, the data subject may at any time withdraw their consent to processing. The controller is required to cease processing of personal data upon the withdrawal of consent. The controller is required to ensure that the ease of withdrawal of consent is comparable to that of giving consent.

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

While there is no specific right to object to the processing of personal data under the DPDPA, the data subject may at any time withdraw their consent to processing. The controller is required to cease processing of personal data upon the withdrawal of consent. The controller is required to ensure that the ease for withdrawal of consent is comparable to that of giving consent.

□ Rights related to automated decision-making, including profiling. What does this right require the organization to do?

The controller is required to ensure that the personal data is complete, accurate, and consistent when the processing of the personal data is likely to be used to make a decision that affects the data subject.

Separately, in addition to the rights set out above, the data subjects have

	the right to: (i) grievance redressal; and (ii) nominate any person to exercise their rights in case of their death or incapacity.

Data Protection Impact Assessments

In what circumstances are data protection impact assessments required?	Data protection impact assessments are only required to be carried out by significant data fiduciaries, once in every 12 (twelve) month period from the date on which a controller is notified as a significant data fiduciary. The following standards have to be adhered to while conducting the data protection impact assessment: a. The data protection impact assessment should contain a description of the rights of the data subjects and the purpose of processing their personal data. b. The data protection impact assessment should contain an assessment and management of the risk to the rights of the data subject. c. The significant data fiduciary should ensure that the person carrying out the data protection impact assessment furnishes a report containing significant observations in the data protection impact assessment to the Data Protection Board.

Data Protection Officer Requirements

Is there a requirement to appoint a DPO? If yes:	The DPDPA does not prescribe a general requirement for all controllers to appoint a data protection officer ("**DPO**"). However, significant data fiduciaries are mandatorily required to appoint a DPO who represents them under the provisions of the DPDPA.
In what circumstances is it required to appoint a DPO?	All significant data fiduciaries, regardless of any threshold, are required to appoint a DPO.
Does the DPO have to possess certain qualifications or meet specific requirements? If so, what are these qualifications or	The DPOs are required to be based in India.

requirements?

What are the responsibilities of a DPO?	DPOs have the following responsibilities under the DPDPA: a. to represent the significant data fiduciary under the provisions of the DPDPA; b. be the individual responsible to the board of directors or similar governing body of the significant data fiduciary; and c. be the point of contact for the grievance redressal mechanism under the provisions of the DPDPA.

Registration

Are there obligations to register with or notify the data protection authority in order to collect or process personal data generally?	No, there is no requirement to register with or notify the data protection authority in order to collect or process personal data.

Security 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 DPDPA imposes the following security controls to protect personal data from unauthorized access, including in respect of any processing undertaken by it or on its behalf by a processor, by taking reasonable security safeguards to prevent personal data breach, which should include, at the minimum: a. appropriate data security measures, including securing of such personal data through its encryption, obfuscation or masking or the use of virtual tokens mapped to that personal data; b. appropriate measures to control access to the computer resources used by such controller or processor; c. visibility on the accessing of such personal data, through appropriate logs, monitoring and review, for enabling detection of unauthorized access, its investigation and remediation to prevent recurrence; d. reasonable measures for continued processing in the event of confidentiality, integrity or availability of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, including by way of data backups; e. for enabling the detection of unauthorized access, its investigation, remediation to prevent recurrence and continued processing in the

event of such a compromise, retain such logs and personal data for a period of 1 (one) year, unless compliance with any law for the time being in force requires otherwise;

f. appropriate provision in the contract entered into between such controller and processor for taking reasonable security safeguards; and
g. appropriate technical and organizational measures to ensure effective observance of security safeguards.

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

A personal data breach under the DPDPA is defined as "*any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data*."

Are there mandatory obligations on the steps an organization is required to take in the event of a data breach / incident?

On becoming aware of any personal data breach, the controller is required to:

a. Notify the occurrence of the personal data breach to each affected data subject, in a concise, clear and plain manner and without delay, through any mode of communication registered by the data subject.
b. Notify to the Data Protection Board:
    i. without delay, with a description of the breach, including its nature, extent, timing and location of occurrence and the likely impact; and
    ii. within 72 *(seventy-two)* hours of becoming aware of the breach, or within such longer period as the Data Protection Board may allow on a request made in writing in this behalf, a notification with the contents as set out in (c)(ii) (*What content must the notification contain*?) 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) – No.

   □ Qualitative threshold (e.g. sensitivity of data or risk posed to data subjects) – No.

b. What are the timing requirements for making a notification?
   The timing requirements for making a notification are as follows:
    i. a notification to each affected data subject – without delay;
    ii. a preliminary notification to the Data Protection Board – without delay; and
    iii. a detailed report including the contents as set out in (c)(iii) (What content must the notification contain?) below – within 72

(seventy-two) hours.

c. What content must the notification contain?
   i. The notification to the data subject must contain: (a) a description of the breach, including its nature, extent and the timing and location of its occurrence; (b) the consequences relevant to the data subject, that are likely to arise from the breach; (c) the measures implemented and being implemented by the controller, if any, to mitigate risk; (d) the safety measures that the data subject may take to protect their interests; and (e) business contact information of a person who can respond on behalf of the controller, to queries, if any, of the data subject.
   ii. The preliminary notification to the Data Protection Board must contain the nature, extent, timing and location of occurrence and the likely impact of the personal data breach.
   iii. The detailed report submitted to the Data Protection Board within 72 (seventy-two) hours must contain: (a) updated and detailed information in respect of a description of the breach; (b) the broad facts related to the events, circumstances and reasons leading to the breach; (c) measures implemented or proposed, if any, to mitigate risk; (d) any findings regarding the person who caused the breach; (e) remedial measures taken to prevent recurrence of such breach; and (f) a report regarding the notifications made to affected data subjects.
d. Are there any other requirements for making notifications?

There are no other requirements for making notifications.

Regulatory Authority and Enforcement

Who is the main data privacy authority or regulator in your jurisdiction?	The Data Protection Board, which is yet to be established by the Central Government, will be the primary data privacy regulator. Separately, any person aggrieved by an order or direction made by the Data Protection Board can approach the appellate tribunal (i.e., the Telecom Disputes Settlement and Appellate Tribunal) for preferring an appeal.
What are the penalties for non-compliance with local data protection laws?	

Failure of the controller to take reasonable security safeguards to prevent a personal data breach.	Up to INR 2,500,000,000 (Indian Rupees Two Billion and Five Hundred Million only) ~USD 29,000,000 (United States Dollars Twenty-Nine Million only)
Failure of the controller to provide the Data Protection Board or affected data subjects notice of a personal data breach.	Up to INR 2,000,000,000 (Indian Rupees Two Billion only) ~USD 23,000,000 (United States Dollars Twenty-Three Million only)
Failure to observe additional obligations in the processing of personal data of children.	Up to INR 2,000,000,000 (Indian Rupees Two Billion only) ~USD 23,000,000 (United States Dollars Twenty-Three Million only)
Failure to observe additional obligations as a notified significant data fiduciary.	Up to INR 1,500,000,000 (Indian Rupees One Billion and Five Hundred Million only) ~USD 17,000,000 (United States Dollars Seventeen Million only)
Failure to adequately observe duties by data subjects.	Up to INR 10,000 (Indian Rupees Ten Thousand only) ~USD 115 (United States Dollars One Hundred and Fifteen only)

Failure to observe any term of a voluntary undertaking submitted by any entity during an inquiry, which has been accepted by the Data Protection Board.	Up to the extent applicable for the contravention in respect of which the proceedings under the procedures to be followed by the Data Protection Board.
Failure to comply with any other provision of the DPDPA or the DPDP Rules.	Up to INR 500,000,000 (Indian Rupees Five Hundred Million only) ~USD 6,000,000 (United States Dollars Six Million only)

Do data subjects have any private remedies?	Yes. Aggrieved data subjects can bring a private action under the DPDPA before the Data Protection Board and may refer an appeal to the Telecom Disputes Settlement and Appellate Tribunal.
Has the data privacy regulator issued any notable enforcement guidance or judgments in the last 12-24 months?	The Data Protection Board under the DPDPA has not been constituted yet. Accordingly, there is no notable guidance or judicial precedent regarding the enforcement of DPDPA.

Associated Contacts

Charmian Aw

Singapore

Email Me

Ciara O'Leary

Singapore

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 it 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.

Definitions

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	Not specifically. However, a data processor's conduct or processing activities is subject to the data controller's instruction.

controllers provide to them?

Legal Bases for 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?

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, and
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 written form or recorded 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 organization to rely on "legitimate interests", what are the relevant requirements or conditions?

- The PDP Law does not further outline what the relevant requirements or conditions are 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 organization 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 organization 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 organization 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 organization to rely on each legal basis mentioned above in 6.a, what are the relevant requirements or conditions?

  Not applicable.

Transparency

Are there any transparency or

Not specifically. However, a data processor's conduct or processing activities is subject to the data controller's instruction.

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?	
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.

Minors' Data

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	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.

children's personal data?	

Direct Marketing, Online Tracking and Cookies

What constitutes direct marketing under the jurisdiction's data protection laws?	PDP Law is silent on this matter. As direct marketing pertains to the use of users' personal data, please see below the requirements.
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. ◦ **Disclosure. What are the requirements for disclosing information to data subjects which are specific to direct marketing or e-marketing?** ◦ **Other requirements. What are the other requirements specific to direct marketing or e-marketing?** None
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 Processor Obligations

Are there any requirements for	Yes, please see our response in point 4 above.

sharing personal data or engaging third party data processors to process personal data?	

Cross-Border Transfers

Are there data localization or similar laws that require personal data to be retained in the local jurisdiction?	Data localization 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 apply. 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 organization 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 Requirements

Is there a requirement to appoint a DPO? If yes:	Yes.

In what circumstances is it required to appoint a DPO?	Data controller and data processor are required to appoint DPO in the event that: 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, it is mandatory to appoint DPO.
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

Are there obligations to register with or notify the data protection authority in order to collect or	No

process personal data generally?

Security 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 unauthorized 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 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

When is a notification obligation triggered:

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

data security breach?	□ 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 of/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 situations the public must also be notified, such as when a failure to inform the public would result in an interference with public services or have a serious impact on the public interest. **Are there any other requirements for making notifications?** The notification form for regulator, i.e. the Ministry of Communication and Digital Affairs, is only available in the Indonesian language. There is no specific format for notification to data subjects. It is considered good practice for all of the notifications, either to the regulator or to the individual, be made available in the Indonesian language.

Regulatory Authority and Enforcement

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.

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

Charmian Aw

Singapore

Email Me

Mochamad Kasmali

Jakarta

Email Me

Teguh Darmawan

Jakarta

Email Me

Andera Rabbani

Jakarta

Email Me

Japan

Last updated 18 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 Japan is the Act on the Protection of Personal Information ("**APPI**").
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)

Definitions

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 Bases for Processing

What are the legal bases	**Consent:**

permitting an organization to collect and process personal data?

(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

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?	◦ 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): ◦ 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.

Minors' Data

Are there specific laws, regulations, rules or guidelines that govern the collection or processing of	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.

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?

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?

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 Marketing, Online Tracking and Cookies

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

- TBA - External Transmission Regulations (so-called cookie rules)
  TBA, Article 27-12

tracking tools?

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 Processor Obligations

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)

Cross-Border Transfers

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 Requirements

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 requirements? If so, what are these qualifications or requirements?	No. However, practically, the DPO should have sufficient knowledge of data protection and data privacy practices in Japan. 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

Are there obligations to register with or notify the data	There is no general legal requirement to register data processing activities nor a requirement to notify the PPC before collecting or processing personal data.

protection authority in order to collect or process personal data generally?	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 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 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 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	Yes.

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

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.

Regulatory Authority and Enforcement

Who is the main data privacy authority or regulator in your jurisdiction?	The Personal Information Protection Commission Japan ("**PPC**").
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).

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

Singapore

Email Me

Hiroto Imai

Tokyo

Email Me

Maria Yaka

Tokyo

Email Me

Mizue Kakiuchi

Tokyo

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.

Definitions

What are the definitions of: (a) personal data,	**a. Provide examples to distinguish between "personal data" and "sensitive personal data."**

and (b) sensitive personal data under data protection laws?	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 defined?	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 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 Bases for Processing

What are the legal bases	**Consent:**

permitting an organization to collect and process personal data?

(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

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	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

the 'Overview of Personal Data Protection Laws' above, or is any additional information required to be covered?	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.

Minors' Data

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 Marketing, Online Tracking and Cookies

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?**

None

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

Not specifically. However, a data processor's conduct or processing activities is subject to the data controller's instruction.

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

Not Applicable

tracking tools?

Data Sharing and Processor Obligations

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.

Cross-Border Transfers

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 Requirements

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

Are there obligations to register with or notify the data protection	No

authority in order to collect or process personal data generally?	

Security 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 data breach / incident?	There are mandatory reporting requirements in cases which trigger such notifications – see our response to sub-question 14.4 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). 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.

Regulatory Authority and Enforcement

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.
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

Charmian Aw

Singapore

Email Me

Sherry Gong

Beijing

Email Me

Flora Feng

Email Me

Jessie Xie

Email Me

Malaysia

Last updated 05 January 2026

Overview of Personal Data Protection Laws

What is the principal legislation, law or regulation governing personal data protection?

In Malaysia, the principal legislation governing personal data protection is the Personal Data Protection Act 2010 ("**PDPA**"), which was passed in 2010 and came fully into force on 15 November 2013, and has since been amended through the Personal Data Protection (Amendment) Act 2024. The PDPA is supported by subsidiary legislation, including the Personal Data Protection Regulations 2013 ("**Regulations**") and accompanying guidelines issued by the Personal Data Protection Commissioner ("**Commissioner**") such as the Guidelines on the Appointment of Data Protection Officer (DPO) ("**DPO Guidelines**") and the Data Breach Notification (DBN) Guidelines ("**DBN Guidelines**").

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

To a limited extent, the PDPA has extra-territorial effect, as it may apply to persons, including companies, established outside Malaysia that use equipment in Malaysia for processing personal data. However, the PDPA generally only applies to personal data processed in Malaysia.

Definitions

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" means any information in respect of commercial transactions, which: (i) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (ii) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (iii) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data controller, including any sensitive personal data and expression of opinion about the data subject.
   b. "Sensitive personal data" means any personal data consisting of information as to the physical or mental health or condition of a

data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence, biometric data or any other personal data as the Minister may determine by order published in the Gazette.

What (if any) exceptions apply to the above definitions of personal data or sensitive personal data?	Under the PDPA, "personal data" expressly excludes any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

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. "Data controller" means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor. b. "Data processor" means any person, other than an employee of the data controller, who processes the personal data solely on behalf of the data controller, and does not process the personal data for any of his own purposes.
Do controllers have any legal obligations to control how processors manage the personal data that the controllers provide to them?	Yes. Where the processing of personal data is carried out by a data processor on behalf of a data controller, the data processor shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction (i) provide sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and (ii) take reasonable steps to ensure compliance with those measures.

Legal Bases for 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? A data controller shall obtain consent from the data subject in relation to the processing of personal data in any form that such consent can be recorded and maintained properly by the data

controller.

b. Does the jurisdiction's data protection law recognize different types of consent?
Yes. While the PDPA does not expressly define "consent", it is generally recognized that consent may be obtained in several ways. "Explicit" consent refers to consent that is clearly and unambiguously given, such as by signing a physical or digital consent form or through an online consent mechanism. "Implied" or "deemed" consent may be inferred from the conduct of the data subject, for example where the individual does not object to the processing after being notified, voluntarily discloses personal data, or proceeds to use the data controller's services. "Verbal" consent may also be valid, provided that it can be evidenced, for instance, through a digital recording or a written confirmation following the verbal consent.

c. Can consent be withdrawn?

Yes. A data subject may withdraw his consent to the processing of personal data by giving a notice in writing to the data controller. Upon receiving the written notice, the data controller shall cease the processing of the personal data.

□ "Legitimate interests":

a. What interests are considered legitimate interests?
The PDPA does not provide for "legitimate interests" as an independent lawful basis for processing personal data. However, it sets out the limited circumstances under which personal data may be processed without the data subject's consent.

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

Not applicable.

□ "Contractual necessity":

a. What purposes would fall under this legal basis?
Under the PDPA, "contractual necessity" allows personal data to be processed without the data subject's consent where the processing is necessary (i) for the performance of a contract; or (ii) for taking steps with a view to entering into a contract.

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

To rely on (i) the data subject must be a party to the contract, and the processing must be necessary for its performance. To rely on (ii) the processing must be necessary to take steps at the request

of the data subject with a view to entering into that contract.

 "Compliance with legal / regulatory requirement":

a. What purposes would fall under this legal basis?
Personal data may be processed without the data subject's consent where the processing is necessary for compliance with any legal obligation.

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

To rely on this basis, the processing must be necessary for compliance with a legal obligation to which the data controller is subject, and that obligation must arise from law other than a contractual obligation.

 Other legal basis apart from the above:

a. What are the other legal bases?
Other legal bases to process personal data without consent include situations where processing is necessary to (i) protect the vital interests of the data subject; (ii) for the administration of justice; or (iii) for the exercise of any functions conferred on any person by or under any law.

b. What purposes would fall under each legal basis mentioned above in 4.a?
The purposes correspond directly to the legal bases described above.

c. For an organization to rely on each legal basis mentioned above in 4.a, what are the relevant requirements or conditions?

To rely on these legal bases, the organization must ensure that the processing is strictly necessary for the specific statutory purpose invoked. In each case, the processing must fall clearly within the scope of the relevant ground and be directly connected to achieving that legitimate statutory objective.

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

Yes.

a. What are the special rules / different legal bases?
The PDPA sets out specific conditions under which sensitive personal data may be processed. A data controller shall not process sensitive personal data except where the data subject has given his explicit consent, or where the processing falls within one of the specific bases, including (i) where the processing is necessary for employment-related legal rights or obligations; (ii) to protect the vital interests of the data subject or another person; (iii) legal

collect or process sensitive personal data?	proceedings; (iv) obtaining legal advice; (v) for establishing, exercising or defending legal rights; (viii) for the administration of justice; (ix) for the exercise of functions conferred by written law; or (xi) for any other purpose as the Minister thinks fit. b. For an organization to rely on each legal basis mentioned above in . (a), what are the relevant requirements or conditions? For an organization to rely on any of the bases, the processing must be strictly necessary for the specific permitted purpose described above.

Transparency

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 data controller is required under PDPA to inform the data subject by written notice, including: (i) that personal data is being processed and provide a description of the personal data to that data subject; (ii) the purposes for which the personal data is being or is to be collected and further processed; (iii) any information available to the data controller as to the source of that personal data; (iv) his right to request access to and to request correction of the personal data; (v) the class of third parties to whom the data controller discloses or may disclose the personal data; (vi) the choices and means the data controller offers for limiting the processing of personal data; (vii) whether it is obligatory or voluntary for the data subject to supply the personal data; and (viii) where it is obligatory to supply the personal data, the consequences for the data subject if he fails to do so.
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. The privacy policy must also include, among others, the following: (i) identify if any sensitive personal data is involved in the processing; (ii) any personal data that the organization is required to collect pursuant to regulator requirement; (iii) the retention period applicable to the processing of the personal data and when such personal data will be disposed of; (iv) the practical measures taken by the organization to ensure the security of personal data; (v) the security measures implemented to ensure that any disclosure of personal data is carried out safely and securely; and (vi) the contact details of the organization's designated Personal Data Protection Officer or person-in-charge (PIC), including the business contact information for handling enquiries or complaints.

Minors' Data

Are there specific laws, regulations, rules or guidelines that govern the collection or processing of children's personal data?	Yes. Where the data subject is under the age of eighteen (18) years, consent shall be obtained from the parent, guardian or person who has parental responsibility under Regulation 3(3).
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? Where the data subject is under eighteen (18) years of age, consent must be obtained from the parent, guardian, or a person who has parental responsibility. This requirement applies to all processing activities involving a minor's personal data.

Direct Marketing, Online Tracking and Cookies

What constitutes direct marketing under the jurisdiction's data protection laws?	"Direct marketing" means the communication by whatever means of any advertising or marketing material which is directed to particular individuals.
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?** An organization may only process personal data for direct marketing purposes where the data subject has given consent. Data subjects also have the statutory right to, at any time, by notice in writing to the data controller, require the data controller to cease or not to begin processing his personal data for purposes of direct marketing. Accordingly, organizations must obtain consent before using personal data for direct marketing and must provide a means for the data subject to give written notice requiring the cessation of such processing at any time. **□ Disclosure. What are the requirements for disclosing information to data subjects which are specific to direct marketing or e-marketing?**

	The PDPA does not prescribe additional disclosure obligations specific to direct marketing, and the general notification requirements apply. Generally, where an organization intends to use personal data for direct marketing or e-marketing, it must disclose this purpose in its written notice and inform data subjects of the choices and means available to cease the processing of their personal data. **□ Other requirements. What are the other requirements specific to direct marketing or e-marketing?** Not applicable.
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 official guidelines in Malaysia that expressly govern the use of cookies or similar online tracking tools. However, where cookies collect information that constitutes personal data, their use generally falls within the scope of the PDPA. In such cases, organizations must obtain the individual's consent for the processing of personal data, provide clear notice of the purposes for which data is collected through cookies, and implement appropriate security measures to protect any personal data collected via these technologies.
What do those laws or guidelines require for the use of cookies or similar online tracking tools?	Not Applicable

Data Sharing and Processor Obligations

Are there any requirements for sharing personal data or engaging third party data processors to process personal data?	Yes. The PDPA imposes specific requirements both for sharing personal data with third parties and for engaging third-party data processors. For the sharing of personal data, the PDPA provides that personal data shall not, without the consent of the data subject, be disclosed for any purpose other than the purpose for which the personal data was collected or a purpose directly related to that purpose, or to any party other than the class of third parties to whom the data controller discloses or may disclose the personal data. A data controller must therefore ensure that disclosure is consistent with the purpose notified and must inform data subjects of the class of third parties to whom their personal data is or may be disclosed.

For the engagement of a third-party data processor, the PDPA requires both the data controller and the data processor to take practical steps to protect the personal data from loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. Further, the data controller must ensure that any data processor appointed provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out and takes reasonable steps to ensure compliance with those measures.

Cross-Border Transfers

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 organization seeking to transfer personal data to rely on such mechanism?
Under Malaysian law, the primary basis for cross-border transfers is where (i) there is in force a law that is substantially similar to the PDPA; or (ii) that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by PDPA.

Separately, the PDPA permits a transfer where the data subject has given his consent to the transfer. To rely on consent, the data controller must ensure that the data subject has been provided with

the written notice and that such consent is capable of being recorded and maintained. Consent must also be voluntary, informed and specific to the cross-border transfer.

b. What if any derogations are permitted by law?

Where the two mechanisms above are not satisfied, the PDPA allows several additional derogations under the PDPA. These derogations permit cross-border transfers in the following circumstances, including: (i) the data subject has given his consent to the transfer; (ii) where the transfer is necessary for the performance of a contract between the data subject and the data controller; (iii) where the transfer is necessary for the conclusion or performance of a contract between the data controller and a third party that is entered into at the request of the data subject or in the interests of the data subject; (iv) where the transfer is required for any legal proceedings, for the purpose of obtaining legal advice, or for establishing, exercising or defending legal rights; (v) where the data controller has reasonable grounds for believing that the transfer is necessary to avoid or mitigate adverse action against the data subject and it is not practicable to obtain the data subject's written consent, but the data subject would have given such consent if it were practicable; (vi) where the data controller has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not, in the destination country, be processed in a manner that would contravene the PDPA if the processing occurred in Malaysia, which may include the use of safeguards such as binding corporate rules, contractual clauses, or certification mechanisms to demonstrate that the receiving party will afford a level of protection consistent with the PDPA; or (vii) where the transfer is necessary in order to protect the vital interests of the data subject.

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?

As set out above, the data controller is required to inform the data subject by written notice that: (i) personal data is being processed and provide a description of the personal data to that data subject; (ii) the purposes for which the personal data is being or is to be collected and further processed; (iii) any information available to the data controller as

to the source of that personal data; (iv) his right to request access to and to request correction of the personal data; (v) the class of third parties to whom the data controller discloses or may disclose the personal data; (vi) the choices and means the data controller offers for limiting the processing of personal data; (vii) whether it is obligatory or voluntary for the data subject to supply the personal data; and (viii) where it is obligatory to supply the personal data, the consequences for the data subject if he fails to do so.

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

The PDPA provides the data subject the right to access personal data that is being processed by or on behalf of the data controller. Upon receiving a written data access request ("**DAR**") together with the prescribed fee, the data controller must inform the requester whether it processes the personal data and, if so, provide a copy of that data in an intelligible form within 21 days from the date of receipt of the DAR. If the data controller is unable to comply within this period, it must issue a written notice explaining the reasons for the delay. The data controller may refuse access only on the specific grounds provided in the PDPA and, where a refusal is made, it must notify the requester in writing within 21 days from the date of receipt of the DAR, stating the reasons for the refusal.

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

The PDPA provides a data subject with the right to request correction of personal data that is inaccurate, incomplete, misleading or not up to date. Upon receiving a written data correction request ("**DCR**"), the data controller must consider whether it is satisfied that the personal data requires correction and, if so, must make the necessary correction and provide the requester with a copy of the personal data within 21 days from the date of receipt of the DCR. The data controller may refuse the request only on the specific grounds provided in the PDPA and, where a refusal is made, it must inform the requester in writing within 21 days from the date of receipt of the DCR, stating the reasons for refusal.

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

The PDPA does not confer a standalone right to erasure or deletion of personal data. However, a data subject may at any time withdraw his consent to the processing of his personal data by giving written notice,

and upon receiving such notice, the data controller must cease processing that personal data. In addition, the data controller must ensure that the personal data shall not be processed if it is no longer necessary for the purpose for which it was collected.

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

Under the PDPA, a data subject has the right to prevent certain processing activities. The data subject may, by written notice, require a data controller to cease or not to begin processing his personal data for a specified purpose or in a specified manner where such processing is causing, or is likely to cause, substantial and unwarranted damage or distress, and the data controller must respond in writing within 21 days stating whether it will comply or give reasons if it considers the notice unjustified.

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

The PDPA provides data subjects the right to data portability. Upon receiving a written request by electronic means from the data subject, the data controller must transmit the data subject's personal data directly to another data controller chosen by the data subject. This obligation applies only where the transmission is technically feasible and where the data formats used by both controllers are compatible. Once a valid request is received, the data controller must complete the transmission of the personal data within the period as may be prescribed.

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

As explained above, under the PDPA, a data subject has the right to prevent certain processing activities. The data subject may, by written notice, require a data controller to cease or not to begin processing his personal data for a specified purpose or in a specified manner where such processing is causing, or is likely to cause, substantial and unwarranted damage or distress, and the data controller must respond in writing within 21 days stating whether it will comply or give reasons if it considers the notice unjustified. Separately, as elaborated above, the PDPA provides a specific right to prevent the use of personal data for direct marketing, enabling the data subject to require the data controller

to cease or not to begin processing his personal data for direct marketing purposes at any time by written notice, and the data controller must act within a reasonable period to cease such processing.

Data Protection Impact Assessments

In what circumstances are data protection impact assessments required?	Malaysia does not currently require organizations to conduct Data Protection Impact Assessments (DPIAs) under the PDPA. While the Commissioner has issued a DPIA Guideline for public consultation, there is no official guideline in force to date.

Data Protection Officer Requirements

Is there a requirement to appoint a DPO? If yes:	Yes. If yes –
In what circumstances is it required to appoint a DPO?	Under the PDPA and the DPO Guidelines, the appointment of a DPO becomes mandatory where the organization's processing activities involve any of the following: i. Personal data exceeding 20,000 data subjects. ii. Sensitive personal data, including financial information exceeding 10,000 data subjects. iii. Activities requiring regular and systematic monitoring of personal data.
Does the DPO have to possess certain qualifications or meet specific requirements? If so, what are these qualifications or requirements?	The DPO Guideline does not impose mandatory professional certifications for a DPO, but it sets out minimum competency expectations that the organization must ensure. A DPO is required to, among others, have knowledge of the PDPA, applicable legal requirements and data-protection practices, together with an understanding of the organization's operations and its personal-data processing activities, as well as familiarity with IT and data-security practices. The DPO must also demonstrate integrity, good corporate-governance awareness and high professional ethics, and be able to promote and cultivate a data-protection culture within the organization. In addition, the Commissioner may require DPOs to undergo specific training programmes or skills-benchmarking mechanisms. The DPO

Guideline further provides that the DPO must be resident in Malaysia or otherwise easily contactable and must be proficient in both Bahasa Melayu and English.

What are the responsibilities of a DPO?

In relation to the organization, the DPO is responsible for informing and advising the organization on its obligations under the PDPA, including assessing personal data processing activities and identifying risk exposure. The DPO must support personal data compliance efforts by advising on issues, among others, internal policies, data-sharing and third-party agreements, and security measures. The DPO should monitor compliance through audits, investigations, training and awareness programmes, and oversee personal data breach and security incident management, including preparing and submitting reports to the Commissioner within the prescribed timelines.

In relation to data subjects, the DPO serves as the primary point of contact for all matters relating to personal data. This includes receiving and managing complaints, handling data-subject rights requests, and providing information regarding the organization's data-processing practices.

In relation to the Commissioner, the DPO acts as the official liaison for regulatory matters. The DPO must facilitate inspections, investigations and requests for information from the Commissioner, ensure accurate and timely regulatory submissions, and represent the organization during engagements with the Commissioner. The DPO Guideline also emphasizes that the DPO must remain independent in the performance of these duties and be supported with adequate resources and direct reporting access to senior management.

Registration

Are there obligations to register with or notify the data protection authority in order to collect or process personal data generally?

No.

Security 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 the PDPA, both data controllers and data processors must take practical steps to safeguard personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. Where a data processor is engaged, the data controller must ensure that the data processor provides sufficient guarantees on technical and organizational security measures and takes reasonable steps to comply with those measures.
How is a "data breach" or "data incident" defined?	Personal data breach" means any breach of personal data, loss of personal data, misuse of personal data or unauthorized access of personal data.
Are there mandatory obligations on the steps an organization is required to take in the event of a data breach / incident?	Yes.
Are there mandatory obligations to notify a regulator or data subjects about a personal data security breach?	Yes. a. **When is a notification obligation triggered:** The notification obligation to the Commissioner is triggered when the personal data breach is considered to cause or is likely to cause "significant harm" if there is a risk that the compromised personal data: □ Quantitative threshold (e.g. volume of data or number of data subjects involved): i. may result in physical harm, financial loss, a negative effect on credit records or damage to or loss of property; ii. may be misused for illegal purposes; iii. consists of sensitive personal data; or iv. consists of personal data and other personal information which, when combined, could potentially enable identity fraud. □ Qualitative threshold (e.g. sensitivity of data or risk posed to data subjects): i. is of significant scale – affected data subjects exceeds one

thousand (1,000).

For data subjects, the same qualitative threshold above applies. However, the significant-scale quantitative threshold does not apply when determining whether notification to affected data subjects is required.

b. **What is the timing requirements for making a notification?**
The organization should notify the Commissioner as soon as practicable and no later than 72 hours from the occurrence of the personal data breach. If the organization cannot meet the 72-hour deadline, it must submit a written explanation with supporting evidence for the delay. Whereas, affected data subjects must be notified without undue delay, and no later than 7 days after the notification to the Commissioner.

c. **What content must the notification contain?**
The notification to the Commissioner must be made in the prescribed notification form provided. The contents required to be provided are set out in the Data Breach Notification Form.

d. **Are there any other requirements for making notifications?**

Yes. The DBN Guidelines impose additional procedural requirements, including, among other, that (i) the notifications to the Commissioner must be submitted using the prescribed format and channels; and (ii) where an organisation notifies affected data subjects, the notification must contain the mandatory information specified in the DBN Guidelines.

Regulatory Authority and Enforcement

Who is the main data privacy authority or regulator in your jurisdiction?	The Personal Data Protection Commissioner.
What are the penalties for non-compliance with local data protection laws?	The PDPA prescribes a range of penalties, depending on the specific provision breached. Offences may attract fines of up to RM1,000,000 or imprisonment of up to three years, or both.
Do data subjects have any private remedies?	While the PDPA is primarily enforced through quasi-criminal offences that may be prosecuted by the authorities, however, data subjects are not limited to regulatory enforcement alone. They may pursue private remedies through civil proceedings, including claims for breach of

confidence, breach of contractual or fiduciary duties of confidentiality, or other applicable common-law causes of action arising from the wrongful disclosure or misuse of their personal data.

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

Yes. A list of compounded cases under the PDPA are published on the PDPC's website.

Associated Contacts

Charmian Aw

Singapore

Email Me

Ciara O'Leary

Singapore

Email Me

Philippines

Last updated 09 December 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 the Philippines is **Republic Act No. 10173** also known as "*Data Privacy Act of 2012*" ("DPA"). In addition to the DPA, the National Privacy Commission ("NPC") also issued the DPA's Implementing Rules and Regulations ("IRR") along with advisories and circulars further regulating personal data processing in the Philippines.

Do the jurisdiction's data

protection laws have extra-territorial scope?

Yes, the DPA provides for extraterritorial application. Under *Section 6 of the DPA*, the Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:

a. The act, practice or processing relates to personal information about a Philippine citizen or a resident.
b. The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:
    1. A contract is entered in the Philippines.
    2. A juridical entity unincorporated in the Philippines but has central management and control in the country.
    3. An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and
c. The entity has other links in the Philippines such as, but not limited to:
    1. The entity carries on business in the Philippines.
    2. The personal information was collected or held by an entity in the Philippines.

Definitions

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

a. Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

Examples of personal data are:

- Names of the owners of condominium units.
- Names and addresses of vehicle owners.
- Image of a person recorded by a camera.
- List of Taxi Operators.
- Contact information such as e-mail, mobile number, and/or landline number.
- Names of health care professionals working in health care institutions.

- **Sensitive personal information** refers to personal information:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations.
2. About an individual's health, education, genetic or sexual life, or any legal proceedings relating to such person.
3. Issued by government agencies peculiar to an individual, including social security numbers, health records, licenses, and tax returns.
4. Specifically established by an executive order or an Act of Congress to be kept classified.

Examples:

- List of names of COVID-19 patients.
- Breath analyzers used on employees and outsourced drivers.
- Medical health information.
- Student transcript of records.
- Driver's license, passport, Social Security ID, and other government-issued IDs.

- The DPA refers to **Privileged Information** as "any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication."

- The IRR refers to personal data as "all types of personal information" which include personal, sensitive personal, and privileged information.

What (if any) exceptions apply to the above definitions of personal data or sensitive personal datas?

Section 4 of the DPA provides for the following exceptions to the application of the law:

a. Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:
    1. The fact that the individual is or was an officer or employee of the government institution.
    2. The title, business address, and office telephone number of the individual.
    3. The classification, salary range, and responsibilities of the position held by the individual.
    4. The name of the individual on a document prepared by the individual in the course of employment with the government.

b. Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract and the name of the individual given in the course of the performance of those services.

c. Information relating to any discretionary benefit of a financial nature, such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit.

d. Personal information processed for journalistic, artistic, literary, or research purposes.

e. Information necessary to carry out the functions of public authority, including the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as amending or repealing Republic Act No. 1405 (Secrecy of Bank Deposits Act), Republic Act No. 6426 (Foreign Currency Deposit Act), and Republic Act No. 9510 (Credit Information System Act).

f. Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510 and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act, and other applicable laws.

g. Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including applicable data privacy laws, which is being processed in the Philippines.

Kindly note that the enumeration in Section 4 does not provide exceptions to the definitions of personal information, sensitive personal information, privileged information, and/or personal data, but only to the application of the DPA. Furthermore, these exceptions do not extend to the requirements of implementing security measures for personal data protection.

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. **Personal Information Controller** ("PIC") refers to a person or organization who controls the collection, holding, processing, or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer, or disclose personal information on his or her behalf.

However, the term ***excludes***:

1. A person or organization who performs such functions as instructed by another

person or organization.
2. An individual who collects, holds, processes, or uses personal information in connection with the individual's personal, family, or household affairs.

- **Personal Information Processor** ("PIP") refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

Do controllers have any legal obligations to control how processors manage the personal data that the controllers provide to them?

Yes. Under the **Principle of Accountability,** each PIC is responsible for personal information under its control or custody, including information that has been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

a. The PIC is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party.
b. The PIC shall designate an individual or individuals who are accountable for the organization's compliance with this Act.

The identity of the individual(s) so designated shall be made known to any data subject upon request.

Furthermore, *Section 14 of the DPA* states that a PIC may subcontract the processing of personal information: provided, that the personal information controller shall be **responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed**, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The PIC shall comply with all the requirements of this Act and other applicable laws.

Legal Bases for 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?**

1. A PIC shall obtain the consent of the data subject in a manner that complies with all the requisites for valid consent.
2. The requisites for valid consent are 1) the consent must be freely

given; 2) specific; 3) informed; 4) an indication of will; and 5) evidenced by written, electronic, or recorded means, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her.

a. As to the first requisite, *Section 7 of NPC Circular No. 2023-04* states that consent is **freely given** when a data subject has a genuine choice and control over their decision to consent to the processing of their personal data.
   Consent is not freely given in instances where there is any element of pressure, intimidation, possibility of adverse consequences for refusal to give consent, or any other inability to exercise free will by the data subject.

b. Under the second requisite, *Section 8 of NPC Circular No. 2023-04* states that a PIC must ensure that the data subject provides specific consent to the specific and declared purposes of the processing of personal data.
   Consent must be granular. In cases where personal data is processed for multiple but unrelated purposes, a PIC shall present to the data subject the list of purposes and allow the data subject to select which purposes they consent to, instead of requiring an all-inclusive consent to the processing for multiple purposes.

c. Regarding the third requisite, *Section 9 of NPC Circular No. 2023-04* states that a PIC should provide to the data subject all relevant information that is necessary for the data subject to make an **informed** decision. Such information must be easily understood by an average member of the target audience to ensure that the data subject has sufficient understanding of what they are consenting to.
   Under *Section 3(A) of NPC Circular No. 2023-04*, the following information should be provided to data subjects in a concise statement: description of the personal data to be processed, the purpose, nature, extent, duration, and scope of processing for which consent is used as basis, the identity of the PIC, the existence of the rights of the data subject, and how these rights can be exercised.

d. With respect to the fourth requisite, *Section 10 of NPC Circular No. 2023-04* requires that consent must be **expressly given through a clear assenting action** that signifies agreement to the specific purposes of the personal data processing as conveyed to the data subject at the time consent was given.
e. Finally, *Section 11 of NPC Circular No. 2023-04* mandates that the consent obtained from a data subject is evidenced by written, electronic, or recorded means. There is no specific

preference among these formats.

b. **Does the jurisdiction's data protection law recognize different types of consent?**

Yes. As previously mentioned under *Section 11 of NPC Circular No. 2023-04*, a PIC must ensure that the consent obtained from a data subject is evidenced by written, electronic, or recorded means. Any of the three formats may be adopted by a PIC.

In addition, consent must be expressly given through a clear assenting action that signifies agreement to the specific purposes of the processing of personal data as conveyed to the data subject at the time consent was given.

A. *Implied consent*. **Consent can never be assumed.** Non-response or implied consent does not constitute valid consent. "Implied consent," for the purposes of this Circular, refers to consent given by action or inaction which is only inferred from the surrounding circumstances when it was given.
B. *Action of the data subject*. Assenting actions are those that indicate agreement to processing activity as described in the information provided by the PIC. A PIC must provide clear information to the data subject on what a particular action means prior to requesting for the data subject's consent.
C. *Continued use of service.* Provided that all the elements of consent are present, and the PIC provides the data subject with information on the processing of personal data for a specific service, the continued use of the PIC's specific service is an assenting action signifying consent.

c. **Can consent be withdrawn?**

Yes. Section 13 of NPC Circular No. 2023-04 permits withdrawal of consent at any time and without cost, subject to limitations provided by law, regulation, or contract. If consent is withdrawn and no other lawful basis justifies continued processing, the PIC must stop processing without undue delay, terminate processing activities (including services relying on that consent), and delete the personal data. Withdrawal does not affect the lawfulness of processing that occurred before withdrawal.

Legitimate interests

a. **What interests are considered legitimate interests?**

While neither the DPA nor NPC Circular No. 2023-07 enumerates or characterizes certain interests as legitimate, the latter provides a

definition of legitimate interest. Specifically, *Section 3(A)* defines legitimate interest as any actual and real interest, benefit, or gain that a PIC or third party may have in or may derive from the processing of specific personal information.[17]

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

The requisites for processing based on legitimate interest are:

a. The legitimate interest is established **(*Purpose Test*)**

A PIC shall determine the existence of a clearly established legitimate interest, including a determination of the objective of the specific processing activity. The purpose of the specific processing activity must be specific, such that it is clearly defined and not vague or overbroad.

The purpose of the specific processing activity must not be contrary to laws, morals, or public policy following the principle of legitimate purpose.

The interest established must be declared to the data subject prior to the processing or at the next practical opportunity, following the principle of transparency and the right of the data subject to be informed.

b. The means to fulfil the legitimate interest is both necessary and lawful **(*Necessity Test*)**

Based on this standard, the means or method chosen for the specific processing activity undertaken to accomplish the legitimate interest of the PIC or the third party should be necessary and lawful. Hence, the means to fulfill the legitimate interest must be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose, in accordance with the principle of proportionality; and must be lawful *i.e.* the PIC cannot violate any law in the process of accomplishing its legitimate interest.

c. The interest is legitimate and lawful, and it does not override fundamental rights and freedoms of data subjects. **(*Balancing Test*)**

A PIC or third party relying on legitimate interest shall determine whether the processing undertaken does not

override the data subject's fundamental rights and freedoms. In doing so, the PIC or third party shall look at the effect or impact of accomplishing the legitimate interest and consider the purpose of processing the interest established and the means by which it is fulfilled.

i. Effect or impact of the specific processing activity on the data subject.
ii. Measures implemented to protect the personal information involved in the specific processing activity or to mitigate the effect or impact of the specific processing activity on the data subject (e.g., privacy-enhancing technologies).
iii. Availability of other means or methods to fulfill the legitimate purpose.
iv. Reasonable expectation of the data subject on the specific processing of their personal information taking into consideration the surrounding circumstances of each case. A PIC shall consider what a reasonable person would find acceptable under the circumstances taking into consideration the interest established.

d. Legitimate interest cannot be relied upon when the processing involves sensitive personal information and privileged information.

 "Contractual necessity". If applicable –

a. **What purposes would fall under this legal basis?**
Under *Section 12(B) of the DPA*, the processing of personal information may be allowed if it is necessary and related to the **fulfillment of a contract** with the data subject or in order to take steps at the request of the data subject prior to entering into a contract. Contractual necessity cannot be relied upon when the processing involves sensitive personal information and privileged information.

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

The data subject must have provided his/her personal information to the PIC. Such collection and processing of such information must be necessary and related to either: 1) the fulfilment of a subsisting contract of which the data subject is a party to; or 2) the fulfilment of a request made by the data subject preparatory to entering into a contract.

 "Compliance with legal / regulatory requirement". If applicable –

a. **What purposes would fall under this legal basis?**
Section 12, paragraphs (c) and (e) of the DPA provide two criteria which may fall under legal/regulatory requirements covering personal information:

   i. The processing is necessary for compliance with a legal obligation to which the PIC is subject.
   ii. The processing is necessary in order to respond to a national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.

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

   With respect to *Section 12(c)*, a PIC must be able to prove that the legal obligation it cites as basis exists and applies to the processing it performed, and that the processing is necessary to comply with the legal obligation. Similarly, under *Section 12(e)*, a PIC must be able to specifically establish the national emergency, requirements of public order and safety, or, in the case of public authority, the mandate supporting such exercise of public authority to support the collection and processing of personal data. Neither criteria can be relied upon when the processing involves sensitive personal information and privileged information.

 Other legal basis apart from the above. If applicable –

a. **What are the other legal bases?**
Apart from paragraphs (a), (b), (c), (e), and (f)*, Section 12 (d) of the DPA* provides for one more criterion for the lawful processing of personal information: the processing is necessary to protect vitally important interests of the data subject, including life and health.

b. **What purposes would fall under each legal basis mentioned above in (a)?**
While the NPC has yet to elaborate on what purposes fall under the concept of vitally important interests of the data subject, the criteria found under Section 12(d) of the DPA clearly provides for the processing of personal information in medical emergencies where the life and/or health of the data subject is at risk.

c. **For an organization to rely on each legal basis mentioned above in (a), what are the relevant requirements or conditions?**
Section 12(d) of the DPA requires that a vitally important interest of

a data subject must be first established before any collection and/or processing of personal information may be justified under this criterion.

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, *Section 13 of the DPA* provides a different set of criteria for the lawful processing of sensitive personal information.

a. **What are the special rules / different legal bases?**
Apart from Consent under paragraph (a), *Section 13 of the DPA* provides the following criteria for the lawful processing of sensitive personal information:

- The processing of the same is provided for by existing laws and regulations: *Provided,* That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further,* That the consent of the data subjects is not required by law or regulation permitting the processing of the sensitive personal information or the privileged information.

- The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing.

- The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: *Provided,* That such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further,* That the sensitive personal information are not transferred to third parties: *Provided, finally,* That consent of the data subject was obtained prior to processing.

- The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured.

- The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the

establishment, exercise or defense of legal claims, or when provided to government or public authority.

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

- **The processing of the same is provided for by existing laws and regulations**

  Section 13(b) of DPA requires a PIC to specifically establish the law and/or regulation relied upon; that such law and/or regulation does not further require the consent of data subjects; and that the law and/or regulation applies to the processing it performed and is necessary for its compliance.

  While Section 12(c) and 13(b) of the DPA appear similar, the former, on the one hand, pertains to all recognized sources of legal obligations as provided under Article 1157 of the Civil Code namely, law, contracts, quasi-contracts, acts or omissions punished by law, and quasi-delicts. On the other hand, the latter specifically pertains to laws and/or regulations, which do not require the consent of data subjects in permitting the processing of sensitive personal information.

- **The processing is necessary to protect the life and health of the data subject or another person**

  Section 13(c) of the DPA requires that the data subject is not legally or physically able to express his or her consent prior to the processing.

- **The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations**

  While the NPC has yet to elaborate on this criterion under *Section 13(d) of the DPA*, the complete language found under this provision requires that the processing be confined and related to only the *bona fide* member of the organization subject of the criterion. Moreover, sensitive personal information processed under this criterion cannot be transferred to third parties. However, it bears noting that the final

requirement/condition of this criterion is that the consent of the data subject be obtained prior to processing which reduces its effectivity as an alternative to consent.

- **The processing is necessary for purposes of medical treatment**
  Processing sensitive personal information for purposes of medical treatment may only be carried out by a medical practitioner or a medical treatment institution. Furthermore, *Section 13(e) of the DPA* requires an adequate level of protection for such data.

- **Necessity for the protection of lawful rights and interests in court proceedings and for the establishment, exercise, or defense of legal claims**

  The qualifier "necessary" in *Section 13(f) of the DPA* pertains to the general privacy principle of proportionality and the requirements of legitimate purpose. The specific processing activity is necessary when it is adequate, relevant, suitable, and not excessive in relation to such legitimate purpose. The specific processing activity must be within the limitations of the law. The phrase "natural or legal persons" under this section refers to persons whose lawful rights and interests are protected in court proceedings, including the parties and their witnesses.

  Processing sensitive personal information based on this criterion may be conducted during the preparatory stages of a prospective case. It does not require that there be an existing proceeding before an administrative agency, court, or other tribunal. Furthermore, processing of personal data based on this criterion need not result in the filing of an actual case and may refer to legal claims of persons other than those who processed the personal data.

Transparency

Are there any transparency or disclosure requirements under the jurisdiction's data protection laws,	Yes. *Section 18 of IRR* provides that the processing of personal data shall adhere to the Principles of Transparency, legitimate purpose, and proportionality.

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

Under *Sec. 16 of the DPA,* a data subject must be furnished the following information before the entry of his or her personal information into the processing system of the PIC, or at the next practical opportunity:

- Description of the personal information to be entered into the system.
- Purposes for which they are being or are to be processed.
- Scope and method of the personal information processing.
- The recipients or classes of recipients to whom they are or may be disclosed.
- Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized.
- The identity and contact details of the personal information controller or its representative.
- The period for which the information will be stored.
- The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

Furthermore, under the **Principle of Transparency,** the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

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

Yes, PICs and PIPs are required to have a privacy policy. However, privacy policies must be distinguished from privacy statements and privacy notices as clarified under NPC Circular No. 2023-04, which provides:

A. *Form.* The following clarifications and distinctions are made on these forms or statements:
   1. *Privacy Statement*. It is a general statement on a PIC's personal data processing practices across the entire organization.
   2. *Privacy Policy*. It is a set of policies that governs a PIC's personal data processing practices. It provides guidance to internal

covered?

relevant parties (*e.g.,* officers, employees) involved in any personal data processing activity. It is also referred to as a "Privacy Manual."

3. *Privacy Notice*. It is a unilateral statement that contains essential information on a specific processing activity of a PIC that involves the data subject. A PIC should use clear and plain language in its privacy notice. Information on how the personal data will be processed must be easily apparent to the data subject. The information should be concrete and definite; provided in the simplest manner possible while avoiding the use of complex sentences or language structures.
   The information enumerated in Q.1 should be in a privacy notice, which, in turn, should be conveyed for the specific processing activity before the processing takes place or at the next practical opportunity.

B. *Consent Form*. It should contain all the information required in a privacy notice and indicate that consent is the lawful criteria for processing relied on. Consequently, it must contain a PIC's proposal to the data subject asking the latter to consent to the processing of personal data pursuant to the terms stated in the consent form. The data subject's acceptance of the provisions of the consent form creates a contract between the data subject and a PIC on the terms of processing of the personal data.
C. *When required.* The requirement of having a privacy statement and notice is separate and distinct from obtaining the consent of the data subject in an appropriate consent form or its equivalent for the lawful processing of personal data.

a. *General rule*. A privacy notice is required in any instance of processing, whether based on consent, other lawful criteria for processing under Sections 12 or 13 of the DPA, or where processing is under a special case pursuant to Section 4 of the DPA.

b. *Exception*. When a consent form already provides the essential information relating to the specific processing activity that enables the data subject to make an informed decision, a separate privacy notice on that specific processing is no longer necessary.

Minors' Data

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

Yes, *NPC Advisory No. 2024-03* provides the Guidelines on Child-Oriented Transparency. These are not legally binding but provide guidance on how DPA should be interpreted and applied in relation to the processing of children's personal data.

personal data?

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

The processing of children's personal data must adhere to the general privacy principles. PICs shall ensure that, in accordance with the Principle of Transparency, children are aware of the nature, purpose, and extent of the processing of personal data.

Consistent with the purpose of a **Privacy Impact Assessment ("PIA")**, PICs shall adopt a risk-based and child-oriented approach when informing children whose data they are processing, taking into account their age and the risks involved in the specific processing activity.

In addition, PICs should implement appropriate measures to address any risks identified in the PIA to ensure the protection of children's personal data taking into consideration the best interests of the child, and to promote the Principle of Transparency in processing activities.

In this regard, PICs may employ the following measures, among others:

1. **Age Assurance Mechanisms.** PICs may implement age assurance mechanisms or solutions to determine the age range of their users as a tool to adopt age-appropriate practices when processing children's personal data. In determining the most suitable age assurance mechanism or solution for a specific processing activity, PICs should recognize that relying solely on users' self-declaration may be inadequate for high-risk processing activities. PICs must ensure that children understand the purpose of the age assurance process. The processing of personal data for age assurance must adhere to the general privacy principles and must have a lawful basis for processing.
2. **Privacy Controls.** PICs must adopt a risk-based approach to determine and implement appropriate and enhanced privacy controls when processing children's personal data, ensuring:
    a. **High Privacy Settings by Default**: Children's accounts must have privacy settings set to the highest level by default. This includes disabling geolocation services, setting profiles to private, and minimizing data sharing unless necessary for the specific purpose.
    b. **Easy Access to Privacy Settings**: PICs must ensure that children are fully aware of the available privacy settings and how to adjust them. These settings should be clear, easy to access, and designed in a way that enables children to understand and control their privacy preferences while maintaining a minimum level of protection.
3. **Privacy Notice**

PICs shall ensure that children are aware of the nature, purpose, and extent of the processing of personal data. PICs should consider the readability (*e.g.*, vocabulary, tone, or style), comprehension, and granularity of privacy notices while taking into consideration the best interests and evolving capacities of children.

PICs shall ensure that privacy notice, including any information and communication relating to the processing of children's personal data, is readily accessible, taking into consideration user experience and user interface.

A. **Content.** PICs should inform the children of the following:
   1. Specific and precise processing activities involving the personal data of the children.

   2. Purpose of processing.

   3. Appropriate lawful basis.

   4. Potential consequences and risks associated with the processing of the personal data of the children.

   5. Importance of privacy settings.

   6. Rights as data subjects and the manner and method of exercising these.

   7. Revisions or updates to the Privacy Notice, if any.

B. **Age-Appropriate Privacy Notice**
   PICs must ensure that any information or communication relating to the processing of children's personal data should be concrete and definitive, and understood by intended or likely users whose personal data are involved in the specific processing activity. PICs shall present the information in a simple manner using clear and plain language while retaining necessary technical terms. This ensures that children receive relevant privacy-related information in a language that is appropriate and easily comprehensible, taking into consideration the age range of the intended or likely users.

   In instances where the product, or service involves or contemplates children as data subjects, regardless of whether it is also intended for adults, PICs must provide child friendly Privacy Notices in addition to standard versions.

C. **Just-in-time Privacy Notice.** PICs shall provide information on how children's personal data will be processed at the point in time when personal data is about to be processed. PICs shall ensure that the information presented is the minimum specific information relevant to the specific processing activity that will be undertaken.
D. **Layered Privacy Notice.** PICs shall use Layered Privacy Notices

that embody the minimum specific information for purposes of the Principle of Transparency. These should direct children to supplemental and detailed information relevant to the specific processing activity that will be undertaken. PICs shall ensure that the supplemental and detailed information presented to children is separate from that intended for adults and presented in a language that is appropriate and easily comprehensible for children.

E. **Deceptive Design Patterns.** PICs shall not use deceptive methods or any form of coercion, compulsion, threat, intimidation, or violence in the processing of the children's personal data. PICs shall not use characters that children know and trust to influence them to provide more information than necessary for the specified and declared purpose. Further, PICs shall not use designs that nudge or steer children toward selecting options that compromise their privacy or are inconsistent with their best interests.

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

Since the processing of children's personal data must adhere to the general privacy principles, the requirements for valid consent on collecting and processing children's personal data is the same as what is provided under the DPA which must be freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

However, the involvement of parents or guardians may be necessary in determining whether children may participate in the specific processing activity, particularly when there are heightened risks to children. PICs must determine the appropriate methods for securing and verifying this involvement based on the level of risk to children.

Direct Marketing, Online Tracking and Cookies

What constitutes direct marketing under the jurisdiction's data protection laws?	The DPA defines Direct Marketing under *Section 3 (d)* as to communication by whatever means of any advertising or marketing material which is directed to particular individuals.

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

□ Consent. If applicable, what are the consent requirements specific to direct marketing or e-marketing?

Processing for direct marketing purposes may require consent in certain instances. Under *Section 14 (B) of NPC Circular No. 2023-04*, a PIC shall obtain the consent of the data subject for direct marketing in cases where the nature of the processing would significantly affect the rights and freedoms of the data subject. However, under *Section 14 (A)* of the said circular, when processing is limited to personal information**,** a PIC may consider direct marketing as a legitimate interest under *Section 12 (f) of the DPA*, during which processing will not require the consent. Nevertheless, a PIC must conduct a legitimate interest assessment under NPC Circular No. 2023-07 to determine the applicability of such criterion. Otherwise, consent will be necessary.

□ Disclosure. If applicable, what are the requirements for disclosing information to data subjects which are specific to direct marketing or e-marketing?

Under the Principle of Transparency, the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

□ Other requirements. If applicable, what are the other requirements specific to direct marketing or e-marketing?

Apart from the DPA, the *Internet Transactions Act of 2023* ("ITA") requires e-marketplaces, in the collection and processing of personal data through e-marketing, to take the necessary precautions to protect the data privacy of consumers, at all times in consonance with the DPA. Moreover, they must comply with the minimum information security standards set by the E-Commerce Bureau, the NPC, and other issuances of relevant government agencies.

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

While there are no specific laws, regulations or guidelines governing the use of cookies and similar online tracking tools, the information processed in relation to the use of such tracking measures is considered personal data and is covered by the DPA. As such, it must still comply with the principles of transparency, legitimate purpose, proportionality

and fairness, and must be supported by the appropriate criteria for the lawful processing of personal data found under Sections 12 and 13 of the DPA.

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

As previously mentioned, while there are no specific laws, regulations or guidelines governing the use of cookies and similar online tracking tools, the information processed in relation to the use of such tracking measures is considered personal data and is covered by the DPA.

Data Sharing and Processor Obligations

Are there any requirements for sharing personal data or engaging third party data processors to process personal data?

Yes, third-party processing of personal data is regulated by the IRR and NPC Circular No. 2020-03. Rule X. Outsourcing and Subcontracting Agreements of the IRR governs processing of personal data by PIPs while NPC Circular No. 2020-03 governs the sharing of personal data between PICs. Compliance with Rule X of the IRR is mandatory while compliance with NPC Circular No. 2020-02 is considered merely directory under NPC Advisory No. 2025-01.

A. **Processing Agreements**

Under *Section 43 of the IRR*, a PIC may subcontract or outsource the processing of personal data to a PIP, provided that contractual or other reasonable means are in place to ensure the confidentiality, integrity, and availability of personal data. Under a processing arrangement, a PIP is considered to be processing for and on behalf of a PIC for purposes that the latter is accountable for. Hence, the PIC remains responsible for ensuring compliance with the privacy principles found under the DPA and is liable for the actions of the PIP as its principal. Hence, disclosures made to PIPs for further processing need not require additional supporting criteria for lawful processing other than those already disclosed by the PIC to its data subject. The PIC, however, pursuant to the principle of transparency, must still inform data subjects of its use of PIPs in pursuit of the purposes already disclosed. The purpose served by the PIP should be sufficient without needing to disclose its identity.

Section 44 of the IRR provides the following mandatory requirements for processing agreements with PIPs:

Processing by a personal information processor shall be governed by a contract or other legal act that binds the personal information processor to the personal information controller.

a. The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the personal information controller, and the geographic location of the processing under the subcontracting agreement.
b. The contract or other legal act shall stipulate, in particular, that the personal information processor shall:

    1. Process the personal data only upon the documented instructions of the personal information controller, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law.
    2. Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data.
    3. Implement appropriate security measures and comply with the Act, these Rules, and other issuances of the Commission.
    4. Not engage another processor without prior instruction from the personal information controller: Provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing.
    5. Assist the personal information controller, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights.
    6. Assist the personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission, taking into account the nature of processing and the information available to the personal information processor.
    7. At the choice of the personal information controller, delete or return all personal data to the personal information controller after the end of the provision of services relating to the processing: Provided, that this includes deleting existing copies unless storage is authorized by the Act or another law.
    8. Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by the personal information controller or another auditor mandated by the latter.
    9. Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission.

B. **Data Sharing Arrangements**

Section 2 (F) of NPC Circular No. 2020-03 defines data sharing as the sharing, disclosure, or transfer to a third party of personal data under the custody of a personal information controller to one or more other PICs. This means that the receiving PIC intends to process the shared personal data for purposes under its independent control and/or supervision not simply for and on behalf of the disclosing PIC.

NPC Circular No. 2020-03 outlines the following requirements for data sharing arrangements:

a. Transparency

Each affected data subject should be provided with the following information before personal data is shared or at the next practical opportunity, through an appropriate consent form or privacy notice, whichever is applicable or appropriate to the lawful basis relied upon:

In cases where consent is not required, a privacy notice is sufficient. Where the PIC has already collected the personal data, it should provide the data subjects with the information above as soon as it decides that personal data will be shared or as soon as possible afterwards.

It is a good practice for PICs to review their privacy notice regularly to ensure that it continues to reflect accurately the data sharing arrangement they are engaged in.

a. Categories of recipients of the personal data: *provided*, that PICs shall provide a data subject with the identity of the recipients, upon request.
b. Purpose of data sharing and the objective/s it is meant to achieve.
c. Categories of personal data that will be shared.
d. Existence of the rights of data subjects.
e. Other information that would sufficiently inform the data subject of the nature and extent of data sharing and the manner of processing involved.

b. Authorized Processing

Data sharing is a form of processing. As with any personal data processing activity, it should be based on any of the criteria for lawful processing under Sections 12 or 13 of the DPA or allowed pursuant to the special cases provided in Section 4 of the DPA.

c. Data Sharing Agreements

While Sections 8 and 9 of NPC Circular No. 2020-03 provide the key considerations for, and prescribed contents of, data sharing agreements ("DSA"), the execution of a DSA is optional under NPC Advisory No. 2025-01. Nevertheless, PICs are encouraged to execute DSAs to demonstrate accountability and good faith in complying with the requirements of the DPA, its IRR, and issuances of the NPC in relation to NPC Circular No. 2020-03. Moreover, the process, decision-making, and steps toward the actual execution of a DSA should facilitate and not hinder lawful data sharing arrangements.

The execution of a DSA is a sound recourse and demonstrates accountable personal data processing, as well as good faith in complying with the requirements of the DPA, its IRR, and issuances of the NPC. The Commission shall take this into account in case a complaint is filed pertaining to such data sharing and/or in the course of any investigation relating thereto, as well as in the conduct of compliance checks.

Cross-Border Transfers

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

There are currently no data localization or similar laws that require personal data to be retained in the Philippines.

What are legal mechanisms for cross-border data transfers ?

There are no special legal mechanisms for cross-border data transfers other than the requirements under Rule XII of the DPA on Accountability. *Section 50* provides:

"Section 50. A personal information controller shall be responsible for any personal data under its control or custody, including information that has been outsourced or transferred to a personal information processor or a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

a. A personal information controller shall be accountable for complying with the requirements of the Act, these Rules, and other issuances of the Commission. It shall use contractual or other reasonable means to provide a comparable level of protection to the personal data while it is being processed by a personal information processor or third party."

Apart from *Rule XII of the DPA, NPC Circular No. 2020-03* and *NPC Advisory No. 2021-02* provide further guidance on cross-border data transfers. The former regulates data sharing arrangement while the latter prescribes the use of the ASEAN model contract clauses and ASEAN data management framework. Neither are mandatory but are considered demonstrations of accountability and good faith compliance with the requirements of the DPA, its IRR, and issuances of the NPC.

 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 data to rely on such mechanism?**
   Not applicable.

b. **What if any derogations are permitted by law?**

   Not applicable.

Data Subject Rights

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

Right to be informed. If applicable, what does this right require the organization to do?

Right to be Informed *(Rule VIII, Section 16 (a) of the IRR)*

1. The data subject has a right to be informed whether personal data pertaining to him or her shall be, are being, or have been processed, including the existence of automated decision-making and profiling.
2. The data subject shall be notified and furnished with information indicated hereunder before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity:

   a. Description of the personal data to be entered into the system.

b. Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose.
c. Basis of processing, when processing is not based on the consent of the data subject.
d. Scope and method of the personal data processing.
e. The recipients or classes of recipients to whom the personal data are or may be disclosed.
f. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
g. The identity and contact details of the personal data controller or its representative.
h. The period for which the information will be stored.
i. The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the Commission.

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

Right to Access *(Rule VIII, Section 16 (c) of the IRR)*

The data subject has the right to reasonable access to, upon demand, the following:

1. Contents of his or her personal data that were processed.
2. Sources from which personal data were obtained.
3. Names and addresses of recipients of the personal data.
4. Manner by which such data were processed.
5. Reasons for the disclosure of the personal data to recipients, if any.
6. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject.
7. Date when his or her personal data concerning the data subject were last accessed and modified.
8. The designation, name or identity, and address of the personal information controller.

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

Right to rectification *(Rule VIII, Section 16 (d) of the IRR)*

The data subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or

otherwise unreasonable. If the personal data has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: *Provided*, That recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject.

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

Right to Erasure or Blocking *(Rule VIII, Section 16 (e) of the IRR)*

The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system.

1. This right may be exercised upon discovery and substantial proof of any of the following:
    a. The personal data is incomplete, outdated, false, or unlawfully obtained.
    b. The personal data is being used for purposes not authorized by the data subject.
    c. The personal data is no longer necessary for the purposes for which they were collected.
    d. The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing.
    e. The personal data concerns private information that is prejudicial to the data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized.
    f. The processing is unlawful.
    g. The personal information controller or personal information processor violated the rights of the data subject.
2. The personal information controller may notify third parties who have previously received such processed personal information.

Right to restrict processing. If applicable, what does this right require the organization to do?

Under *Section 11 of the DPA*, when the personal information is inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.

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

Right to Data Portability

The Right to Data Portability is provided under *Section 36 of the IRR*, where his or her personal data is processed by electronic means and in a structured and commonly used format, the data subject shall have the right to obtain from the personal information controller a copy of such data in an electronic or structured format that is commonly used and allows for further use by the data subject. The exercise of this right shall primarily take into account the right of the data subject to have control over his or her personal data being processed based on consent or contract, for commercial purpose, or through automated means. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

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

Right to Object (Section 34 [b])

The data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph. When a data subject objects or withholds consent, the personal information controller shall no longer process the personal data, unless:

1. The personal data is needed pursuant to a subpoena.
2. The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject.
3. The information is being collected and processed as a result of a legal obligation.

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

The DPA provides that a data subject shall have reasonable access to, upon demand, information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject.

No decision with legal effects concerning a data subject shall be made solely on the basis of automated processing without the consent of data subjects.

Data Protection Impact Assessments

In what circumstances are data protection impact assessments required?

A PIP and PIC shall conduct a PIA on the processing of personal data: Provided, that such assessment shall be updated as necessary (e.g., new features or major changes in processing, new regulations, new contracts entered by the PIC, or changes in its PIP). Both previously assessed controls and those newly identified through recent PIAs shall be monitored, evaluated, updated, and incorporated as a component of a PIC's Privacy Management Program.

In general, a PIA should be undertaken for every processing system of a PIC or PIP that involves personal data. It may also be carried out vis-à-vis the entire organization of the PIC or PIP with the involvement or participation of the different process owners and stakeholders. *NPC Advisory 2017-03* provides the prescribed guidelines for the conduct of PIAs.

Children's Personal Data

A PIA is required when children's personal data is involved. PICs must incorporate Child Privacy Impact Assessments ("CPIA") as part of their PIAs before launching products or services intended or likely to be accessed by children and thereafter as may be necessary. The PIA is a continuing requirement, regularly reviewed and updated to account for changes in products, services, processes, or regulations. The factors that must be considered include, but are not limited to:

1. Purpose of processing.
2. Types of data to be processed (e.g., collected, used, or disclosed).
3. Sources of data.
4. Systems to be used (e.g., open or closed systems).
5. Data storage and disposal.
6. Data sharing.
7. Security measures implemented.
8. Effect or impact of the specific processing activity on children.
9. Age range of intended or likely users.
10. Process owner for the specific processing activity of the PIC or PIP.
11. Risk Identification.
12. Involvement of Parents or Guardians.

References

- 36. Sec. 4 (d), NPC Circular No. 2023-06 on Security of Personal Data in the Government and the Private Sector.
- 37. NPC Advisory No. 2017-03.
- 38. Sec. 2 (A), NPC Advisory No. 2024-03.

Data Protection Officer Requirements

Is there a requirement to appoint a DPO? If yes:	*NPC Advisory No. 2017-01* requires that a Data Protection Officer shall be designated. A PIC or PIP shall designate an individual or individuals who shall function as DPO. The DPO shall be accountable for ensuring compliance by the PIC or PIP with the DPA, its IRR, issuances by the NPC, and other applicable laws and regulations relating to privacy and data protection.
In what circumstances is it required to appoint a DPO?	It shall apply to all natural or juridical persons, or any other body in the government or private sector engaged in the processing of personal data within and outside of the Philippines, subject to the applicable provisions of the DPA, its IRR, and issuances by the NPC.
Does the DPO have to possess certain qualifications or meet specific requirements? If so, what are these qualifications or requirements?	Yes. The DPO should possess specialized knowledge and demonstrate reliability necessary for the performance of his or her duties and responsibilities. As such, the DPO should have expertise in relevant privacy or data protection policies and practices. He or she should have sufficient understanding of the processing operations being carried out by the PIC or PIP, including the latter's information systems, data security and/or data protection needs. Knowledge by the DPO of the sector or field of the PIC or PIP, and the latter's internal structure, policies, and processes is also useful. The minimum qualifications for a COP shall be proportionate to his or her functions, as provided in this Advisory.[40]
What are the responsibilities of a DPO?	A DPO shall: a. Monitor the PIC's or PIP's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. b. Ensure the conduct of PIAs relative to activities, measures, projects, programs, or systems of the PIC or PIP. c. Advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data). d. Ensure proper data breach and security incident management by

the PIC or PIP, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period.

e. Inform and cultivate awareness on privacy and data protection within the organization of the PIC or PIP, including all relevant laws, rules and regulations and issuances of the NPC.
f. Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach.
g. Serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP.
h. Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security.
i. Perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.

Registration

Are there obligations to register with or notify the data protection authority in order to collect or process personal data generally?

Yes.

a. What are these obligations and their timing requirements?

Registration

In compliance with *NPC Circular No. 2022-04* effective 11 January 2022, all applications for registration of Data Processing System and Data Protection Officer shall be through the NPC Registration System ("NPCRS") only.

Mandatory Registration

Not all entities are required to create an account with the NPCRS. Under Section 5 of NPC Circular No. 2022-04, a PIC/PIP shall be required to register under the online platform when ANY of the following are present:

a. PIC or PIP employing two hundred fifty (250) or more persons.
b. PIC or PIP processing sensitive personal information of one thousand (1,000) or more individuals.
c. PIC or PIP processing data that will likely pose a risk to the rights and freedoms of data subjects Government Agency or Instrumentality (Government processing will likely pose a risk to the rights and freedoms of data subjects).

Voluntary Registration

An application for registration by a PIC or PIP processing personal data who does not operate under any of the conditions set forth under Section 5 of NPC Circular No. 2022-04, the PIC or PIP may register voluntarily.

Section 47 of the IRR provides for the contents of registration:

1. The name and address of the personal information controller or personal information processor, and of its representative, if any, including their contact details.
2. The purpose or purposes of the processing, and whether processing is being done under an outsourcing or subcontracting agreement.
3. A description of the category or categories of data subjects, and of the data or categories of data relating to them.
4. The recipients or categories of recipients to whom the data might be disclosed.
5. Proposed transfers of personal data outside the Philippines.
6. A general description of privacy and security measures for data protection.
7. Brief description of the data processing system.
8. Copy of all policies relating to data governance, data privacy, and information security.
9. Attestation to all certifications attained that are related to information and communications processing.
10. Name and contact details of the compliance or data protection officer, which shall immediately be updated in case of changes.

Entities for mandatory registration with a new DPS must register within twenty (20) days from the launch of the system.

Entities who are required to register must register the appointment or designation of a new DPO within twenty (20) days from the designation or Appointment.

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

Yes. A personal information controller or personal information processor that employs fewer than two hundred fifty (250) persons shall not be required to register unless the processing it carries out is likely to pose a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive personal information of at least one thousand (1,000) individuals.

Security and Breach Notification

What obligations

A. **Data Privacy and Security**

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

1. PIC and PIP shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data.
2. PICs and PIPs shall take steps to ensure that any natural person acting under their authority and who has access to personal data, does not process them except upon their instructions, or as required by law.
3. The security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing. These measures shall be implemented to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

B. **Organizational Security Measures**

Where appropriate, PICs and PIPs shall comply with the following guidelines for organizational security:

a. **Compliance Officers.** Any natural or juridical person or other body involved in the processing of personal data shall designate an individual or individuals who shall function as data protection officer, compliance officer or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security.

b. **Data Protection Policies.** Any natural or juridical person or other body involved in the processing of personal data shall implement appropriate data protection policies that provide for organizational, physical, and technical security measures, and, for such purpose, take into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects.

    1. The policies shall implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself.
    2. The policies shall implement appropriate security measures that, by default, ensure only personal data which is necessary for the specified purpose of the processing are processed. They shall determine the amount of personal data collected, including the extent of processing involved, the period of their storage, and their accessibility.

3. The polices shall provide for documentation, regular review, evaluation, and updating of the privacy and security policies and practices.

c. **Records of Processing Activities.** Any natural or juridical person or other body involved in the processing of personal data shall maintain records that sufficiently describe its data processing system, and identify the duties and responsibilities of those individuals who will have access to personal data. Records should include:

   1. Information about the purpose of the processing of personal data, including any intended future processing or data sharing.
   2. A description of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing.
   3. General information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data.
   4. A general description of the organizational, physical, and technical security measures in place.
   5. The name and contact details of the personal information controller and, where applicable, the joint controller, its representative, and the compliance officer or Data Protection Officer, or any other individual or individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.

d. **Management of Human Resources.** Any natural or juridical person or other entity involved in the processing of personal data shall be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data.

   The said employees, agents, or representatives shall operate and hold personal data under strict confidentiality if the personal data are not intended for public disclosure. This obligation shall continue even after leaving the public service, transferring to another position, or upon terminating their employment or contractual relations. There shall be capacity building, orientation or training programs for such employees, agents or representatives, regarding privacy or security policies.

e. **Processing of Personal Data.** Any natural or juridical person or other body involved in the processing of personal data shall develop, implement and review:

1. A procedure for the collection of personal data, including procedures for obtaining consent, when applicable.
2. Procedures that limit the processing of data, to ensure that it is only to the extent necessary for the declared, specified, and legitimate purpose.
3. Policies for access management, system monitoring, and protocols to follow during security incidents or technical problems.
4. Policies and procedures for data subjects to exercise their rights under the Act.
5. Data retention schedule, including timeline or conditions for erasure or disposal of records.

f. **Contracts with Personal Information Processors.** The personal information controller, through appropriate contractual agreements, shall ensure that its personal information processors, where applicable, shall also implement the security measures required by the Act and these Rules. It shall only engage those personal information processors that provide sufficient guarantees to implement appropriate security measures specified in the Act and these Rules and ensure the protection of the rights of the data subject.

C. **Physical Security Measures**

Where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for physical security:

a. Policies and procedures shall be implemented to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media.

b. Design of office space and workstations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public.

c. The duties, responsibilities and schedule of individuals involved in the processing of personal data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or workstation, at any given time.

d. Any natural or juridical person or other body involved in the processing of personal data shall implement policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of personal data.

e. Policies and procedures that prevent the mechanical destruction of files and equipment shall be established. The room and workstation used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

D. **Technical Security Measures**

Where appropriate, personal information controllers and personal information processors shall adopt and establish the following technical security measures:

a. A security policy with respect to the processing of personal data.

b. Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network.

c. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services.

d. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach.

e. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

f. A process for regularly testing, assessing, and evaluating the effectiveness of security measures.

g. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.

E. **Appropriate Level of Security**

The Commission shall monitor the compliance of a natural or juridical person or other body involved in the processing of personal data, specifically their security measures, with the guidelines provided in these Rules and subsequent issuances of the Commission. In determining the level of security appropriate for a particular personal information controller or personal information processor, the Commission shall take into account the nature of the personal data that requires protection, the risks posed by the processing, the size of the organization and complexity of its operations, current data privacy best practices, and the cost of security implementation. The security measures provided herein shall be subject to regular review and evaluation and may be updated as necessary by the Commission.

F. **Security of Personal Data in the Government and the Private Sector (NPC Circular No. 2023-06)**

Under Section 32 of NPC Circular No. 2023-06, the PIC or a PIP shall continuously adapt security measures to respond to the evolving security threat landscape. This includes identifying threats based on authoritative sources of threat information, integrating relevant threats into the PIA to determine if these lead to new unacceptable security or privacy risks, and proposing corrective actions to such threats.

Passwords

To maintain the security of the personal data from unauthorized access, all personal data that are processed must be adequately protected through industry standards and best practices. Each PIC or PIP shall issue and enforce a Password Policy.

PICs shall also implement secure authentication mechanisms, such as multifactor authentication or secure encrypted links, when providing personnel online access to sensitive personal information, privileged information, and a high volume of personal data.

Authorized Devices

PICs shall ensure that only known devices, properly configured to the PIC's or PIP's security standards, are authorized to access personal data. The PIC or PIP shall also establish solutions that only allow authorized media to be used on its computer equipment. These measures include but are not limited to:

1. setting a group policy to allow certain types of devices to be connected;
2. use of endpoint security solutions;

3. restricting access to USB ports.

Mobile Devices

PICs shall employ technology solutions that enable remote disconnection or data deletion on mobile devices owned by the PIC when they are lost or compromised. In addition, PICs shall establish a notification process in cases of mobile device loss to ensure swift and appropriate actions toward safeguarding personal data contained therein.

Business Continuity Plan

A PIC or PIP must have a Business Continuity Plan to mitigate potential disruptive events. It must consider:

Personal data backup, restoration, and remedial time;

a. Periodic review and testing of the business continuity plan which takes into account disaster recovery, privacy, business impact assessment, crisis communications plan, and telecommuting policy;

b. Contact information and other business-critical matters, e.g., electrical supply, building facilities, Information and Communications Technology (ICT) assets.

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

Personal data breach refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:

1. an availability breach resulting from loss, accidental or unlawful destruction of personal data;

2. integrity breach resulting from alteration of personal data; and/or

3. a confidentiality breach resulting from the unauthorized disclosure of or access to personal data.

Security incident is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It shall include incidents that would result in a personal data breach, if not for safeguards that have been put in place.

References

- 53. Sec. 3 (F), NPC Circular 16-03.

- 54. Sec. 3 (J), NPC Circular 16-03.

Are there mandatory obligations on the steps an organization is required to take in the event of a data breach / incident?

Yes, the *NPC Circular 2023-06* requires PICs to notify the NPC and the affected data subjects upon knowledge of, or when there is reasonable belief that a personal data breach has occurred. All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. Any or all reports shall be made available when requested by the Commission: provided that a summary of all reports shall be submitted to the Commission annually, comprised of general information including the number of incidents and breach encountered, classified according to their impact on the availability, integrity, or confidentiality of personal data.

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

- Yes. In case of Personal Data Security breach the PIC shall notify the NPC and the data subject.

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

- **a. When is a notification obligation triggered:**
- Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:

A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.
B. There is reason to believe that the information may have been acquired by an unauthorized person.
C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

b. □ Quantitative threshold (e.g. volume of data or number of data subjects involved) – 500 or more.

There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject.

- **c. □ Qualitative threshold (e.g. sensitivity of data or risk posed to data subjects) – Likely to cause significant harm**

to an affected individual.

There shall also be no delay in the notification if the breach involves the disclosure of sensitive personal information that will harm or adversely affect the data subject.

- **d. What are the timing requirements for making a notification?**

Notification of Data Subject

The PIC shall notify the data subjects affected by a personal data breach within seventy-two (72) hours upon receiving knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.[59] Except in cases when it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification.

Notification of the NPC

The PIC shall notify the NPC of a personal data breach within seventy-two (72) hours upon receiving knowledge of or the reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.

- **e. What content must the notification contain?**

Notification of the Data Subject

The notification shall include, but not be limited to:

1. nature of the breach;

2. personal data possibly involved;

3. measures taken to address the breach;

4. measures taken to reduce the harm or negative consequences of the breach;

5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and

6. any assistance to be provided to the affected data subjects.

Notification to the Commission

The notification shall include, but not be limited to:

1. Nature of the Breach

a. description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;

b. a chronology of the events leading up to the loss of control over the personal data;

c. approximate number of data subjects or records involved;

d. description or nature of the personal data breach;

e. description of the likely consequences of the personal data breach; and

f. name and contact details of the data protection officer or any other accountable persons.

2. Personal Data Possibly Involved

a. description of sensitive personal information involved; and

b. description of other information involved that may be used to enable identity fraud.

3. Measures Taken to Address the Breach

a. description of the measures taken or proposed to be taken to address the breach;

b. actions being taken to secure or recover the personal data that were compromised;

c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;

d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;

e. the measures being taken to prevent a recurrence of the incident.

The Commission reserves the right to request additional information, if necessary.

- **f. Are there any other requirements for making**

notifications?

- Yes. The PICs shall cooperate with the NPC where there is an investigation related to the breach. The requirements pertaining to notification and the submission of reports shall also be complied with through the appropriate submissions to the office of the National Privacy Commission or by electronic mail (complaints@privacy.gov.ph).

Regulatory Authority and Enforcement

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

The main data privacy authority or regulator in the Philippines is the National Privacy Commission ("**NPC**").

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

Rule XIII of the IRR provides for the penalties in case of non-compliance of the Data Privacy laws.

A. Unauthorized Processing of Personal Information and Sensitive Personal Information (Section 52)

a. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under the Act or any existing law.
b. A penalty of imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process sensitive personal information without the consent of the data subject, or without being authorized under the Act or any existing law.

B. Accessing Personal Information and Sensitive Personal Information Due to Negligence (Section 53)

a. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under the Act or any existing law.
b. A penalty of imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to sensitive personal information without being authorized under the Act or any existing law.

C. Improper Disposal of Personal Information and Sensitive Personal Information (Section 54)

a. A penalty of imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00) shall be imposed on persons who knowingly or negligently dispose, discard, or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.
b. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the sensitive personal information of an individual in an area accessible to the public or has otherwise placed the sensitive personal information of an individual in its container for trash collection.

D. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes (Section 55)

a. A penalty of imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under the Act or under existing laws.
b. A penalty of imprisonment ranging from two (2) years to seven (7) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under the Act or under existing laws.

E. Unauthorized Access or Intentional Breach (Section 56)

A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information are stored.

F. Concealment of Security Breaches Involving Sensitive Personal Information (Section 57)

A penalty of imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f) of the Act, intentionally or by omission conceals the fact of such security breach.

G. Malicious Disclosure (Section 58)

Any personal information controller or personal information processor, or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or sensitive personal information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

H. Unauthorized Disclosure (Section 59)

a. Any personal information controller or personal information processor, or any of its officials, employees, or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).
b. Any personal information controller or personal information processor, or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

I. Combination or Series of Acts *(Section 60)*

Any combination or series of acts as defined in Sections 52 to 59 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).

J. Extent of Liability *(Section 61)*

If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. Where applicable, the court may also suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and he or she is found guilty of acts penalized under Sections 54 and 55 of these Rules, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.

K. Large-Scale *(Section 62)*

The maximum penalty in the corresponding scale of penalties provided for the preceding offenses shall be imposed when the personal data of at least one hundred (100) persons are harmed, affected, or involved, as the result of any of the above-mentioned offenses. Section 63. Offense Committed by Public Officer. When the offender or the person responsible for the offense is a public officer, as defined in the Administrative Code of 1987, in the exercise of his or her duties, he or she shall likewise suffer an accessory penalty consisting of disqualification to occupy public office for a term double the term of the criminal penalty imposed.

Do data subjects have any private remedies?

Yes. A data subject may file a complaint in the NPC in case of violation this Act. Section 64 of the IRR provides that pursuant to the exercise of its quasi-judicial functions, the Commission shall award indemnity to an aggrieved party on the basis of the provisions of the New Civil Code. Any complaint filed by a data subject shall be subject to the payment of filing fees, unless the data subject is indigent.

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 https://privacy.gov.ph/.

For Advisories:

1. NPC Advisory No. 2025-02: Guidelines On Privacy Engineering In Systems Life Cycle Processes
2. NPC Advisory No. 2025-01: Clarification on Certain Provisions of NPC Circular No. 2020-03 on Data Sharing Agreements
3. NPC-IC Joint Advisory No. 2025-001: Considerations on the Use of Privacy Enhancing Technologies (PETs) in the Insurance Industry
4. NPC Advisory No. 2024-04: Guidelines on the Application of Republic Act

No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations, and the Issuances of the Commission to Artificial Intelligence Systems Processing Personal Data
5. NPC Advisory No. 2024-03: Guidelines on Child-Oriented Transparency - FAQ Guidelines on Child-Oriented Transparency
6. NPC Advisory No. 2024-02: Guidelines on Personal Data Processing Based on Section 13 (f) of the Data Privacy Act of 2012
7. NPC Advisory No. 2024-01: Model Contractual Clauses for Cross-Border Transfers of Personal Data
8. NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns

For Circulars:

1. NPC Circular No. 2025-01 - Guidelines on the Processing of Personal Data Collected Using Body-Worn Cameras
2. NPC Circular No. 2024-02 - Closed-Circuit Television (CCTV) Systems
3. NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission
4. NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest
5. NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector - FAQ Security of Personal Data in the Government and the Private Sector
6. NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program - FAQ Prerequisites for the Philippine Privacy Mark Certification Program
7. NPC Circular No. 2023-04 - Guidelines on Consent
8. NPC Circular No. 2023-03 - Guidelines on Identification Cards
9. NPC Circular No. 2023-02 - Data Privacy Competency Program - FAQ Data Privacy Competency Program
10. NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission

Associated Contacts

Charmian Aw

Singapore

Email Me

Ciara O'Leary

Singapore

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.

Definitions

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 Bases for 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

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?	

Minors' Data

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 Marketing, Online Tracking and Cookies

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 Processor Obligations

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.

Cross-Border Transfers

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 Requirements

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

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

Security 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.

Regulatory Authority and Enforcement

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	

penalties for non-compliance with local data protection laws?	
Do data subjects have any private remedies?	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

Singapore

Email Me

Ciara O'Leary

Singapore

Email Me

South Korea

Last updated 02 November 2025

Overview of Personal Data Protection Laws

What is the principal legislation, law or regulation governing personal data	The Personal Information Protection Act (PIPA). It was enacted in 2011, and its most recent major amendment, aimed at centralizing the data protection framework and aligning with global standards, came into effect on September 15, 2023.

protection?

Do the jurisdiction's data protection laws have extra-territorial scope?	PIPA does not contain a single blanket "extra-territoriality" article, but foreign business operators may fall within PIPA when they provide goods/services to, or otherwise process personal information of, data subjects in South Korea, and they can be required to designate a domestic agent in South Korea. (PIPC, Guidelines on Applying the PIPA to Foreign Business Operators, Apr. 4, 2024; PIPA Art. 31 2)

Definitions

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."** i. Personal data is defined as information relating to a living individual that falls under any of the following: (1) Information by which an individual can be identified, such as a name, resident registration number, or image; (2) Information that, even if it cannot identify a specific individual by itself, can be easily combined with other information to do so. Whether information can be "easily combined" is determined by reasonably considering the time, cost, and technology required to identify the individual, including the availability of the other information; (3) Information that has been pseudonymized per (1) or (2) and cannot identify a specific individual without the use or combination of additional information for restoration (pseudonymized information) (*PIPA* Art. 2(1)). ii. Sensitive personal data is defined as personal information that could markedly invade an individual's privacy, including information on ideology, beliefs, trade union or political party membership, political views, health, sex life, and other personal information prescribed by Presidential Decree. The Presidential Decree further specifies genetic information, biometric information for uniquely identifying an individual, racial or ethnic information, and criminal records as sensitive data (*PIPA* Art. 23; Enforcement Decree Art. 18). As a rule, processing sensitive data requires the data subject's separate and explicit consent.
What (if any) exceptions apply to the above definitions of personal data or sensitive personal data?	*PIPA* does not carve out a general "business contact information" exemption from the scope of "personal information." Rather, anonymized information that irreversibly cannot identify an individual falls outside *PIPA*, and pseudonymized information is subject to special rules that permit use for statistics, scientific research, etc., under separate safeguards (*PIPA* Art. 2(1) & Chapter on Pseudonymized Information Arts. 28-2 to 28-7).

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 "personal information controller" is a person (individual, corporate or otherwise) who, alone or jointly, determines the purposes and methods of processing personal information. (PIPA Art. 2(5)) PIPA does not use the term "processor" in the GDPR sense,but regulates entrusted processing (delegation) where a controller entrusts handling to a trustee (subcontractor). (PIPA Art. 26(1)).
Do controllers have any legal obligations to control how processors manage the personal data that the controllers provide to them?	When entrusting processing, the controller must execute a written contract specifying purpose/scope, technical–administrative safeguards, prohibition of out-of-purpose use, re-entrustment conditions, inspection, and supervision of the trustee; the controller remains responsible for compliance. (PIPA Art. 26(1)–(3))

Legal Bases for Processing

What are the legal bases permitting an organization to collect and process personal data?	Processing is lawful if one of the following applies: (i) data subject consent; (ii) contractual necessity; (iii) legal obligation; (iv) protection of vital interests (life, body, property) where urgent; (v) processing by a public institution to perform its statutory duties; or (vi) processing necessary for the legitimate interests of the controller where such interests are not overridden by data subject rights/interests and the processing remains within a reasonable scope. (PIPA Art. 15(1)1–6) **Consent:** (a) What are the conditions or requirements for obtaining valid consent? Controllers must inform data subjects of prescribed matters before collection/use (e.g., purpose, items, retention, right to refuse and disadvantages) and obtain opt-in consent by methods allowed under PIPA; bundling consent beyond what is necessary for a service is restricted. (PIPA Arts. 15(2), 22(1)–(5), 17(2) for third-party provision). (b) Does the jurisdiction's data protection law recognize different types of consent?

The PIPA distinguishes between consent for collection/use, consent for third-party provision, consent for processing sensitive data, and consent for receiving marketing information, and requires that data subjects be able to consent to each item separately (PIPA Arts. 22(2)).

(c) Can consent be withdrawn?

Data subjects may request suspension of processing or otherwise withdraw consent, and controllers must accommodate this without undue delay. (PIPA Art. 37(1)–(4))

□ "Legitimate interests":

(a) What interests are considered legitimate interests?

The PIPA permits the use or provision of personal data without consent "where it is necessary to achieve the legitimate interests of the personal information controller, which clearly override the rights of the data subject." This basis is interpreted narrowly and applies only under strict conditions. (PIPA Art. 15(1)6)

(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?

Processing necessary to conclude or perform a contract with the data subject is permitted. (PIPA Art. 15(1)2)

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

The processing must be necessary for the contract; controllers should not force consent where another legal basis (e.g., contract) suffices for core service features. (PIPA Arts. 15(1)2, 22(5))

□ "Compliance with legal/regulatory requirement":

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

Processing necessary to comply with law is permitted. (PIPA Art. 15(1)3)

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

The processing must be required or permitted by the relevant statute/regulation. (PIPA Art. 15(1)3)

□ Other legal basis apart from the above:

	(a) What are the other legal bases? PIPA recognizes: public-institution tasks (for public bodies); vital interests (urgent life/body/property protection); additional use/provision "reasonably related" to original purpose with safeguards; and pseudonymized-information processing for statistics/scientific research, etc. (PIPA Arts. 15(1)4–5, 15(3), 18(2), 28-2 to 28-7) (b) What purposes would fall under each legal basis mentioned above in (a)? Examples include public duties by authorities, emergency medical needs, compatible further use where criteria are met (e.g., low risk, safeguarding), and research using pseudonymized data. (PIPA Arts. 15(1)4–5, 15(3), 28-2 to 28-7) (c) For an organization to rely on each legal basis mentioned above in (a), what are the relevant requirements or conditions? "Additional use/provision" must consider the relation to original purpose, feasibility of identifiability removal, safeguards, and impact on data subjects; pseudonymized-data use must follow PIPA's dedicated safeguards. (PIPA Arts. 15(3), 28-2 to 28-7)
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?	Processing sensitive information requires separate, explicit consent or a statutory ground; resident registration numbers (RRNs) are separately restricted and generally cannot be processed based on consent alone (legal basis or vital-interest emergency required), with encryption mandated. (PIPA Arts. 23(1), 24-2(1)–(2))

Transparency

Are there any transparency or disclosure requirements under the jurisdiction's data protection laws,	What are the items of information that must be disclosed to data subjects? Controllers must establish and disclose a Privacy Policy that is easily recognizable and continuously updated, covering purpose(s) of processing, items collected, retention period, third-party provision,

requiring disclosure of certain information to data subjects? If yes – what are the items of information that must be disclosed to data subjects?	processing of pseudonymized information (if any), rights/exercise methods, safeguards, domestic agent (if designated), and privacy officer (DPO/CPO) contact. (PIPA Art. 30(1)–(2); Enforcement Decree Art. 31(2))
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?	Are organizations required to have a privacy policy? The Privacy Policy must include all required items (above) and be made public (e.g., website), including the business contact of the privacy officer and, where applicable, of the domestic agent. (PIPA Art. 30(2); PIPA Art. 31(1)–(2); PIPA Art. 31-2(3))

Minors' Data

Are there specific laws, regulations, rules or guidelines that govern the collection or processing of children's personal data?	Yes; for children under 14, when consent is the legal basis, controllers must obtain legal representative (parent/guardian) consent and verify it; notices to children must use clear and simple language. (PIPA Art. 22-2(1)–(2))
What mandatory requirements do those laws, regulations, rules or guidelines provide for the collection or processing of children's personal data?	Legal-representative consent is required before processing a child's personal information; controllers may collect minimum information from the child solely to obtain the representative's consent (e.g., parent's name/contact) and must design child-friendly notices. (PIPA Art. 22-2(3)–(4))

Direct Marketing, Online Tracking and Cookies

What constitutes direct marketing under the jurisdiction's data protection laws?	PIPA does not define "direct marketing," but using contact details (phone/email/SMS, etc.) to send promotional messages constitutes processing and triggers PIPA obligations if personal information is involved. (PIPA Art. 2(1))
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 under PIPA is generally required for third-party provision or for using personal information for marketing beyond what is necessary for the service, and separate/opt-in consent is expected for promotions. (PIPA Arts. 15(1)1, 17(1)–(2), 22(1)–(5)) Separately, the Network Act imposes strict rules on electronic advertising (e.g., labeling, opt-out, and night-time restrictions for unsolicited messages, typically 9:00 PM–8:00 AM, unless there is prior consent). (Network Act Art. 50) **□ Disclosure. What are the requirements for disclosing information to data subjects which are specific to direct marketing or e-marketing?** When sending marketing messages, the term "(□□)" [Ad] must be displayed at the beginning of the message. The sender's name, contact details, and a clear method for opting out must also be included (The Network Act Art. 50). **□ Other requirements. What are the other requirements specific to direct marketing or e-marketing?** Transmissions must cease immediately if a recipient opts out, and the recipient cannot be charged for doing so (Article 50, Paragraph 6 of the Network Act). Furthermore, sending marketing messages between 9:00 PM and 8:00 AM requires separate prior consent (The Network Act Art. 50).
What specific laws, regulations or guidelines (if any) govern the use of cookies and similar online tracking tools?	Yes, the Network Act and the PIPA are relevant.
What do those laws or guidelines require for the	

use of cookies or similar online tracking tools?	If cookies or other tracking tools identify an individual (alone or in combination), their use constitutes the processing of personal information; controllers must notify data subjects of such purposes and obtain consent where required, and the Privacy Policy must describe the installation/operation and refusal of automatic collection devices (e.g., cookies). (PIPA Art. 30(1)-(2)) In addition, the PIPC has issued policy directions on online behavioral advertising, emphasizing clear notice, choice, and accountability for profiling-based ads. (PIPC policy direction on online behavioral advertising, 2024)

Data Sharing and Processor Obligations

Are there any requirements for sharing personal data or engaging third party data processors to process personal data?	Third-party provision of personal information generally requires separate consent with prescribed disclosures (recipient, purpose, items, retention, right to refuse and disadvantages). (PIPA Art. 17(1)–(2)) Entrusted processing must be under a written contract and accompanied by supervision and public disclosure of the fact of entrustment (e.g., in the Privacy Policy). (PIPA Art. 26(1)–(3))

Cross-Border Transfers

Are there data localization or similar laws that require personal data to be retained in the local jurisdiction?	PIPA imposes no general data localization rule, though sector-specific laws (e.g., certain mapping/geospatial, financial or location-information regimes) may impose constraints. (PIPA generally; sectoral practice) (PIPA Art. 28-8 framework).
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.

- □ Entrustment/storage necessary to conclude or perform a contract with the data subject.

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

- Consent: Before obtaining consent, inform the data subject of: items to be transferred; destination country; transfer date/method; recipient's name/contact; recipient's purpose and retention period; and how to refuse and the effects of refusal. Changes to any of these require renewed consent. (PIPA Art. 28-8(2)–(3))
- Adequacy ("equivalence") decision: Transfers are permitted where the PIPC recognizes the destination's regime as substantially equivalent. Note: On September 16, 2025, the PIPC recognized the EU as equivalent (in force that day). (PIPA Art. 28-8(1)5; PIPC/EU announcements) On September 16, 2025, the PIPC granted its first equivalence recognition to the European Union (EU), confirming that the EU provides a level of protection comparable to that under the PIPA.
- Certification mechanisms: Permitted where the overseas recipient holds a PIPC-recognized certification and takes mandated safety/rights-guarantee measures and implements certified matters locally. As of 2025, no data transfer certification mechanisms have yet been designated or recognized by the PIPC. (PIPA Art. 28-8(1)4(a)–(b))
- Entrustment/storage necessary for contract performance: If entrusting processing and retaining data overseas is necessary to conclude or perform a contract with the data subject, transfers may proceed without consent, provided that the items listed in Art. 28-8(2) are: (i) disclosed in the Privacy Policy; or (ii) individually notified by prescribed means (e.g., email). (PIPA Art. 28-8(1)3, (1)3(a)–(b))

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

Transfers may occur without consent if required by a specific law/treaty or for the imminent protection of the life, body, or property of a data subject or third party. (PIPA Art. 28-8(1)2; Art. 18(2))

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?**
  Provide clear notice at the time of data collection and maintain an accessible public Privacy Policy.
- **Right of access. What does this right require the organization to do?**
  On request, provide a data subject with a copy of their personal data within 10 days or a legally valid reason for refusal.
- **Right to rectification. What does this right require the organization to do?**
  Promptly correct any inaccurate personal data upon the data subject's request and inform them of the result.
- **Right to erasure. What does this right require the organization to do?**
  On request, destroy personal data that is no longer necessary or was processed unlawfully, and notify the data subject.
- **Right to restrict processing. What does this right require the organization to do?**
  Cease processing a data subject's information upon their request, unless a compelling legal basis to continue exists.
- **Right to data portability. What does this right require the organization to do?**
  On request, provide personal data in a machine-readable format for transfer to the data subject or another organization, where technically feasible.
- **Right to object.**What does this right require the organization to do?
  While PIPA does not have a distinct right titled "Right to object," the Right to restrict processing described above provides a similar function, allowing data subjects to effectively object to the ongoing processing of their data.

- **Rights related to automated decision-making, including profiling. What does this right require the organization to do?**

  Allow data subjects to refuse, request an explanation, or seek human intervention for significant decisions made solely by automated means.

Data Protection Impact Assessments

In what circumstances are data protection impact assessments required?	Under PIPA, public institutions must conduct a personal information impact assessment for certain high-risk personal information files and submit results to PIPC; no statutory DPIA applies generally to private-sector controllers under PIPA. (PIPA Art. 33(1), (8))

Data Protection Officer Requirements

Is there a requirement to appoint a DPO? If yes:	Every controller must designate a privacy officer who oversees PIPA compliance. (PIPA Art. 31(1))
In what circumstances is it required to appoint a DPO?	The designation obligation applies broadly to all controllers processing personal information in South Korea. (PIPA Art. 31(1))
Does the DPO have to possess certain qualifications or meet specific requirements? If so, what are these qualifications or requirements?	Yes. All personal information controllers must designate a Privacy Officer (sometimes referred to as a DPO/CPO). The requirements differ depending on the size of the organization: a. General requirement (all controllers): The Privacy Officer must be an executive-level individual (or equivalent status) within the organization. They are responsible for establishing and implementing privacy management plans, conducting internal inspections, handling data subject complaints and remedies, responding to incidents, and ensuring staff training and compliance. b. Additional requirements for large-scale processors: If a controller: (i) processes the personal information of ≥ 1,000,000 data subjects, or (ii) generated at least KRW 10 billion (approx. USD 7.5 million) in the previous fiscal year from personal-information-related activities, stricter qualification standards apply. In such cases, the Privacy Officer must have relevant expertise and experience in data protection or information security. This may be demonstrated through: Professional work experience in personal data protection or information security; Academic qualifications in a relevant field;

	or Recognized professional certifications (e.g., attorney with data protection practice, information security credentials). (Enforcement Decree Art. 32(1)–(3))
What are the responsibilities of a DPO?	The privacy officer's duties include establishing a privacy plan, monitoring processing practices, handling complaints/remedies, internal controls, training, file management, and immediate corrective measures upon violations, with protection from unjust disadvantage. (PIPA Art. 31(2)-(5))

Registration

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

Security 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?	Controllers must take necessary technical/administrative/physical measures to ensure security and prevent loss, theft, leakage, alteration or damage of personal information. (PIPA Art. 29)
How is a "data breach" or "data incident" defined?	PIPA uses the term "divulgence, loss, or theft" (commonly translated as "leakage, etc.") to cover unauthorized disclosure or loss events involving personal information. (PIPA Art. 34(1))
Are there mandatory obligations on the steps an	Controllers must notify affected data subjects without delay and report to PIPC/KISA if thresholds are met; maintain records and take remedial measures. (PIPA Art. 34(1)-(3))

organization is required to take in the event of a data breach / incident?

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

For regulator notifications and data subject notifications respectively:

Both notifications to data subjects and reports to the competent authority may be required, but the triggers differ.

(a) When is a notification obligation triggered:

 Quantitative threshold (e.g., volume of data or number of data subjects involved) – *1,000 or more*.

 Qualitative threshold (e.g., sensitivity of data or risk posed to data subjects) – *likely to cause significant harm to an affected individual.*

To the regulator (PIPC/KISA): Required if any of the following apply:

- the breach affects 1,000 or more data subjects;
- the breach involves sensitive personal information or unique identifiers (e.g., resident registration numbers); or
- the breach results from unauthorized external access (e.g., hacking).

To data subjects: Required whenever any leakage, loss, or theft of personal information occurs, regardless of the number of data subjects.

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

Notification must be made without undue delay and within 72 hours of becoming aware of a breach. *(PIPA Art. 34; Enforcement Decree Art. 39)*

(c) What content must the notification contain?

Standard notifications include what happened, items compromised, timing, remedial steps, contact points, and additional items per PIPC format. *(PIPA Art. 34(1)–(3))*

(d) Are there any other requirements for making notifications?

Controllers must maintain records of the incident and measures taken. Controllers must cooperate with follow-up orders from the PIPC/KISA (e.g., corrective measures, further reporting).

Regulatory Authority and Enforcement

Who is the main data privacy authority or regulator in your jurisdiction?	South Korea's independent authority is the Personal Information Protection Commission (PIPC). (PIPA Art. 7(1))
What are the penalties for non-compliance with local data protection laws?	PIPA provides for administrative surcharges/fines (including up to 3% of total sales revenue, excluding unrelated revenue), corrective orders, and criminal penalties for certain offenses. (PIPA penalty framework including Arts. 64, 75; amended 2023)
Do data subjects have any private remedies?	Aggrieved individuals can bring civil claims (including punitive damages in specified cases) and seek injunctive relief under PIPA and the Civil Act. (PIPA damages/relief provisions; general civil remedies)
Has the data privacy regulator issued any notable enforcement guidance or judgments in the last 12-24 months?	PIPC has emphasized: (i) breach response and ransomware preparedness; (ii) cross-border compliance and domestic-agent accountability; and (iii) online tracking/behavioral advertising transparency, reflected in notable orders and surcharges against well-known platforms and large domestic service providers.

Associated Contacts

Charmian Aw

Singapore

Email Me

Ciara O'Leary

Singapore

Email Me

Thailand

Last updated 17 December 2025

Overview of Personal Data Protection Laws

What is the principal legislation, law or regulation governing personal data protection?	The main legislation governing data protection in Thailand is the Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**").
Do the jurisdiction's data protection laws have extra-territorial scope?	**Yes.** The PDPA has an extraterritorial effect, whereby the data controller and data processor, who are not in Thailand, would also be obligated to comply with the provisions of the PDPA if the processing involves: ◦ Offering of goods or services to the data subjects in Thailand, regardless of whether payment is made by the data subjects or not. ◦ Monitoring of the behavior of the data subjects that takes place in Thailand.

Definitions

What are the definitions of: (a) personal data, and (b) sensitive personal data under data protection laws?	Personal data is broadly defined as any data pertaining to an individual that enables the identification of such an individual, whether directly or indirectly, but excluding data of a deceased person. The PDPA does not define nor refer to the term "**sensitive personal data**". However, Section 26 of the PDPA provides a list of personal data that is subject to heightened requirements in terms of legal bases for the personal data processing, as the processing of such personal data could result in greater harm and penalties in case of breach. This list of personal data under Section 26 is substantially similar to the list of the special categories of personal data under the General Data Protection Regulation ("**GDPR**"), i.e. personal data pertaining to ethnicity, race, political opinions, doctrinal, religious or philosophical beliefs, sexual behavior, criminal records, health information, disability, labor union, genetic data, biometric data, or any other data which may affect the data subject in the same manner as prescribed by the Personal Data Protection Committee ("**PDPC**").

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?	**Yes.** ◦ "**Data Controller**" means a person or legal entity who has the power to determine the collection, use, or disclosure ("**processing**" or "**process**") of personal data. ◦ "**Data Processor**" means a person or legal entity who processes personal data on behalf, or pursuant to the instructions, of the data controller.
Do controllers have any legal obligations to control how processors manage the personal data that the controllers provide to them?	**Yes.** Where a data controller engages a data processor, the data controller must have in place an agreement with the data processor to ensure that the data processor processes personal data in accordance with its obligations under the PDPA ("**Data Processing Agreement**").

Legal Bases for 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? Under the PDPA, consent will only be valid and legally binding on the data subject if the consent request is made in accordance with the PDPA. These consent request requirements are as follows: ◦ **Form:** Consent request must be made in writing or through electronic means, unless impossible due to its nature. ◦ **Characteristics:** The consent request must: (a) inform the data

subject of the purpose for which consent is required; (b) be clearly separated from other parts; (c) use plain language; (d) be clear and not be misleading or deceptive as to the purpose; (e) be easily understandable and accessible; and (f) not be conditional upon the entering into the contract or provision service which is not necessary or relevant.

- **Manner:** Freedom of the data subject in giving consent must be taken into utmost consideration when requesting for consent. Therefore, consent must be freely and affirmatively given, reflecting the data subject's true intention (e.g., through ticking a checkbox or clicking an accept button).
- **Timing:** Consent request must be made before or at the time of collecting, using, or disclosing personal data.

b. Can consent be withdrawn?

Yes. Generally, a data subject has the right to withdraw consent at any time, and the data subject must be able to withdraw consent as easily as when giving consent. The withdrawal of consent would not affect the lawfulness of the processing of personal data which has been carried out by the data controller prior to such withdrawal.

 "Legitimate interests"

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

The processing of personal data may rely on the legitimate interests' legal basis when it is necessary for the legitimate interests of the data controller or any other person or juristic person, and such interests is not overridden by the fundamental rights or freedoms of the data subject.

 "**Contractual necessity"**

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

When it is necessary for the performance of contractual obligations to which the data subject is a party, or to take steps at the request of the data subject, prior to entering into a contract.

 "Compliance with legal/regulatory requirement"

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

Under the PDPA, there are no additional requirements specified for relying on this legal basis, apart from the fact that the processing is for the compliance with a legal obligation to which the data controller is subject.

Other legal bases apart from the above:

a. What are the other legal bases?

Research & statistics, vital interests, and public interest.

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

Please refer to the table below for more details.

From the above questions, the details of the other legal bases are summarized in the following table.

Research & Statistics	To achieve the purpose relating to the preparation of historical documents or archives for public interest, or it is related to research or statistics, in which appropriate measures are implemented, to protect the rights and freedoms of the data subjects.	Suitable measures to safeguard the data subject's rights and freedoms are put in place and in accordance with the notification ~~as~~ prescribed by the PDPC.
Vital Interests	To prevent or suppress danger to the life, body, or health of a person.	**N/A.**

Public Interest	When it is necessary for the performance of tasks which are carried out by the data controller in the public interest, or it is necessary for the exercise of an official authority vested in the data controller.	**N/A.**

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. The PDPA recognizes the concept of "sensitive personal data" under Section 26 as discussed earlier. For sensitive personal data, explicit consent is generally required, unless the processing falls within the exemption, e.g., for preventing or suppressing a danger to a person's life, body or health where a data subject cannot give consent; when it is necessary for compliance with specific laws, etc.

Transparency

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

Yes. The data controller must notify the data subject of the following information prior to, or at the time of collection of his/her personal data ("**Notification Requirement**"):

i. Purposes of the processing of the personal data.
ii. Circumstances where personal data is required for the compliance with the law, or performance of a contract, or is necessary to proceed with the data subject's request to enter into a contract, as well as consequences for not providing personal data under said circumstances.
iii. Personal data to be collected.
iv. Retention period, or if a specific retention period cannot be set, the expected retention period according to the data retention standard.
v. Types of persons/entities that the personal data will be disclosed to.

to data subjects?	vi. Information and contact details of data controller and, where applicable, local representative and/or data protection officer ("**DPO**"). vii. The rights of the data subject under the PDPA.
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.** Organizations acting in the capacity of data controller must comply with the Notification Requirement. This is usually done in the form of a privacy notice or policy.

Minors' Data

Are there specific laws, regulations, rules or guidelines that govern the collection or processing of children's personal data?	No.
What mandatory requirements do those laws, regulations, rules or guidelines provide for the collection or processing of children's personal data?	The method for obtaining consent, and the consent form, must also comply with the requirements stipulated under the PDPA. Please refer to the "Legal basis for collection and processing" above for more details. According to the PDPA, if a data subject is a minor ("**minor data subject**") and he/she is more than 10 years old but below 20 years old, unless legally married pursuant to the terms of the Civil and Commercial Code ("**CCC**"), parental consent is also required together with the minor's consent themselves, except for transactions they have legal capacity under the CCC in which case, only minor's consent is required. In the case where the minor data subject is not exceeding 10 years old, consent for the processing of personal data of the minor is required to be obtained from the parent or legal guardian only, without any exemptions.

Direct Marketing, Online Tracking and Cookies

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

The PDPA does not define "direct marketing", but under Direct Sales and Direct Marketing Act, B.E. 2545 (2002), it is defined as the marketing of goods and services by communicating information for the purpose of offering the sale of goods or services directly to a consumer who is located far away from the operator, with the intention that each consumer responds and purchases the goods or services from the direct marketing business operator.

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 provisions governing the use of personal data for direct marketing or e-marketing under the PDPA. If consent needs to be obtained, it must comply with the consent requirements mentioned in the "Legal basis for collection and processing" above.

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

There are no specific provisions governing the use of personal data for direct marketing or e-marketing under the PDPA. If consent needs to be obtained, it must comply with the consent requirements mentioned in the "Legal basis for collection and processing" above.

□ Other requirements. If applicable, what are the other requirements specific to direct marketing or e-marketing?

The Ministerial Notification on the Characteristics and the Method of Sending Data Deemed Not Causing a Disturbance to the Recipient B.E. 2560 (2017), which was issued by virtue of the Computer Crime Act B.E. 2560 (2017) (as amended) stipulates that sending marketing communication via email is generally regarded as the act causing disturbance to the recipient, unless (a) consent has been obtained from the recipient for the sending of such marketing communication; and (b) each marketing communication sent to the recipient contains mark, detail and procedure for which the recipient can easily opt-out/unsubscribe from receiving such communication.

What specific laws, regulations

or guidelines (if any) govern the use of cookies and similar online tracking tools?	Currently, the PDPA does not have any specific provision on the use of cookies and other similar online tracking tools (collectively, the "**cookies**"). Nonetheless, in the event that cookies will be used to collect personal data, such use will be subject to the provisions of the PDPA.
What do those laws or guidelines require for the use of cookies or similar online tracking tools?	Where cookies will be used to collect personal data, implementation of a cookies banner and cookies policy is advisable due to the following reasons: ◦ The PDPA requires the data controller to notify the data subject of the Notification Requirement prior to or at the time of collection of personal data. ◦ The PDPA only permits the processing of personal data if there is a legal basis, and where consent is required for the processing, the consent request must, among others, be made prior to or at the time of processing.

Data Sharing and Processor Obligations

Are there any requirements for sharing personal data or engaging third party data processors to process personal data?	**Data Controller and Data Processor** Where the data controller engages the data processor, the data controller must have in place a Data Processing Agreement with the data processor to ensure that the data processor will process personal data in accordance with its obligations under the PDPA. Currently, the notifications of the PDPC only require the data controller to ensure that the Data Processing Agreement includes an obligation of the data processor to notify the data controller of the personal data breach incident within 72 hours upon becoming aware of such breach, and to implement appropriate security measures as prescribed by the notification of the PDPC. **Data Controller and Data Controller** The PDPA does not prescribe that there must be an agreement in place between data controllers and data controllers; however, it does impose an obligation that where the data controller discloses personal data to any third party, the data controller is obligated to ensure that such third party will not use or disclose such personal data without authorization

or unlawfully. Therefore, it is advisable that there should nevertheless be an agreement in place to govern the sharing/disclosure of personal data (e.g. Data Sharing Agreement).

Cross-Border Transfers

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

No. The PDPA does not impose data localization or mandatory retention requirements. However, under the Notification of the National Cybersecurity Committee Re: Guideline for the Use of Public Cloud Service having Data Centre in Thailand B.E. 2567 (2024), government agencies, regulators, and critical information infrastructure (CII) entities using public cloud services must host primary and backup data centers in Thailand if their systems are classified as high impact. Backups abroad are allowed only in United Nations member jurisdictions, such as Singapore or the Hong Kong SAR. It is also important to note that certain industry-specific regulations may mandate data localization requirements.

What are legal mechanisms for cross-border data transfers ?

 Data subject consent.

 Transfers to jurisdictions that 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 data to rely on such a mechanism?

The PDPA generally permits the cross-border transfer of personal data by the data controller to a destination country or international organization that has adequate personal data protection standards ("**Whitelisted Countries**") as prescribed by the PDPC. Currently, the PDPC has not yet announced the list of Whitelisted Countries. Cross-

border transfer of personal data is nevertheless permitted if personal data is transferred by the data controllers under any of the following circumstances:

- To comply with the law.
- The data subject is informed of the inadequacy of the destination country or international organization and grants consent to the cross-border transfer.
- It is necessary to perform contractual obligations of a contract of which the data subject is a party, or to proceed with the request for the data subject before entering into such a contract.
- It is to perform contractual obligations of a contract between the data controller and other persons for the interests of the data subject.
- For vital interests.
- For public interests.

In addition to the above, the PDPA also permits the cross-border transfer of personal data where personal data is transferred overseas by the data controller or data processor within the same group of undertakings to jointly operate the business ("**Affiliated Entities**"), provided that a personal data protection policy for the cross-border transfer of personal data among such Affiliated Entities ("**Binding Corporate Rules**" or "**BCR**") must be examined and certified by the Office of the PDPC. Alternatively, personal data can be transferred if appropriate safeguard is implemented in accordance with the Notification of the PDPC Re: Criteria For the Protection of Personal Data Sent or Transferred to a Foreign Country Pursuant to Section 29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023) ("**BCRs and Appropriate Safeguards Notification**"). Appropriate safeguards can be done in the form of, among other things, contractual clauses which can either be drafted by including the provisions required under the BCRs and Appropriate Safeguards Notification; or can be adopted from other recognized contractual clauses, e.g. the ASEAN Model Contractual Clauses for Cross Border Data Flows or the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries which are issued by virtue of the GDPR. Such clauses must however contain the provisions required by the BCRs and Appropriate Safeguards Notification.

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?

Organizations must comply with the Notification Requirement prior to or at the time of collection of personal data. This is usually done in the form of a privacy notice or policy. Please refer to the "Transparency/disclosure requirements" above for more details.

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

The data subject has the right to request access to personal data, and obtain a copy of their personal data, as well as to request the disclosure of how personal data has been acquired by the data controller without consent. In general, the data controller must comply with the data subject request within 30 days of receipt.

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

A data subject has the right to request that his/her personal data be rectified so that it would be accurate, up-to-date, complete, and not misleading.

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

A data subject has the right to request the data controller to erase, destroy, or de-identify personal data in certain circumstances such as when the personal data is no longer necessary for the purposes for which it was processed, when a data subject has withdrawn their consent for the processing of personal data, etc. In general, the data controller is required to comply with a data subject's request within 90 days of receipt.

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

A data subject has the right to request that the use of personal data be suspended under certain circumstances, such as where the data subject requested to exercise the right to rectification, and the data controller is in the process of examining such request, etc.

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

The data subject has the right to request to have personal data in the format which is generally readable and usable by automatic tools or devices and which can be disclosed and used by automatic means, and to request that personal data in said format be transmitted to another data controller, as well as to request to obtain the personal data in the format that the data controller sends or transmits to another data controller.

□ Right to object. what does this right require the organization to o?

The data subject has the right to object to the processing of personal data, for example, where the data controller processes personal data for direct marketing purposes. Upon receipt of the objection request, the data controller must cease processing the relevant personal data and promptly segregate the objected data from other data sets.

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

N/A.

Data Protection Impact Assessments

In what circumstances are data protection impact assessments required?	**No.** Data protection impact assessments (DPIA) are not statutorily mandated in Thailand.

Data Protection Officer Requirements

Is there a requirement to appoint a DPO? If yes:	**Yes.**
In what circumstances is it required to appoint a DPO?	The data controller and the data processor must designate a DPO in any of the following circumstances: i. where the data controller or the data processor is a public authority as

prescribed by the PDPC;

ii. where the activities of the data controller or the data processor in the processing of the personal data require regular monitoring of the personal data or the system, by reason of having a large scale of personal data as prescribed by the PDPC; or

iii. where the core activity of the data controller or the data processor is the processing of sensitive personal data.

The appointment of the DPO must be notified to the Office of the PDPC using the prescribed form.

Does the DPO have to possess certain qualifications or meet specific requirements? If so, what are these qualifications or requirements?

No. Currently, the PDPA does not specify any formal qualifications for the DPO.

What are the responsibilities of a DPO?

The tasks of the DPO under the PDPA are summarized below:

- Provide guidance regarding the compliance with the PDPA to the data controller or data processor, as well as the data controller or data processor's employees and service providers (collectively, the "**Personnel**").
- Investigate the performance of the data controller or data processor and the Personnel with respect to the processing of personal data to ensure compliance with the PDPA.
- Coordinate and cooperate with the Office of the PDPC where issues arise with respect to the processing of personal data by the data controller or data processor and Personnel in accordance with the PDPA.
- Maintain confidentiality of the personal data the DPO has acquired or knows due to the performance of the DPO's tasks under the PDPA.

Registration

Are there

obligations to register with or notify the data protection authority in order to collect or process personal data generally?	**No.**

Security 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 the PDPA, the data controller is required to implement appropriate security measures to protect personal data, which must at least meet the minimum standard stipulated by the PDPC under the Notification Re: Requirements of Security Measures for Data Controllers B.E. 2565 (2022) ("**Notification on Security Measures**"). Furthermore, the data controller must require its data processor to implement appropriate security measures as prescribed by the Notification on Security Measures. The security measures must be periodically reviewed by the data controller when it is necessary, or when the technology has changed, in order to efficiently maintain the appropriate security and safety.
How is a "data breach" or "data incident" defined?	The Notification of the PDPC Re: Rules and Procedures for the Personal Data Breach Notification ("**Data Breach Notification**") defines "personal data breach" as any breach of security that leads to loss, or unauthorized or unlawful access, use, change, alteration, or disclosure of personal data, whether such breach occurs intentionally, willfully, by negligence, without authorization or unlawfully, computer crime, cyber threat, any mistake, accident, or any other reasons.
Are there mandatory obligations on the steps an organization is required to take in the event of a data breach / incident?	**Yes.** The Data Breach Notification stipulates that when the data controller has been notified of the personal data breach or becomes aware of the personal data breach or the suspected personal data breach, the data controller is to, among others, assess to determine whether the information is reliable, as well as the assessment of the risk of the personal data breach.
Are there mandatory obligations to	

notify a regulator or data subjects about a personal data security breach?

Yes. The Data Controller is obligated to notify the Office of the PDPC of the personal data breach, unless the personal data breach does not have a risk of affecting the rights and freedoms of an individual. If the personal data breach has ***a high risk of affecting the rights and freedoms of an individual***, apart from notifying the Office of the PDPC, the data controller must also notify the affected data subject.

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).

   The Data Breach Notification stipulates the factors to be taken into consideration when assessing the risk of a personal data breach such as nature type, and volume of personal data involved, severity of the consequences of the data breach incident, etc.

b. What are the timing requirements for making a notification?
   Timeline to notify the Office of the PDPC: Without delay and, as far as feasible, within 72 hours upon becoming aware of the personal data breach.

   Timeline to notify the Data Subject: Where the personal data breach has a high risk of affecting the rights and freedoms of individuals, the data controller must notify the Office of the PDPC as described above and must also notify the affected data subjects of such incident, together with the remedial actions, without delay.

c. What content must the notification contain?
   Notify the Office of the PDPC: When notifying the PDPC Office of a personal data breach, the data controller must, to the extent possible, include: (i) a brief description of the breach, including categories and number of affected data subjects or records; (ii) the name and contact details of the DPO (if appointed) or designated contact person; (iii) information on possible impacts arising from the breach; and (iv) details of measures taken or planned to prevent, mitigate, or remedy the incident.

   Notify the Data Subject: When notifying affected data subjects, the data controller must, to the extent possible, include: (i) a brief description of the breach; (ii) the name and contact details of the DPO (if appointed) or designated contact person; (iii) information on possible impacts to the individual; and (iv) guidance on remedial actions and a summary of the measures taken or planned to prevent, mitigate, or remedy the incident.

d. Are there any other requirements for making notifications?

No.

Regulatory Authority and Enforcement

Who is the main data privacy authority or regulator in your jurisdiction?	The Office of the Personal Data Protection Committee is the regulator of the PDPA.
What are the penalties for non-compliance with local data protection laws?	Non-compliance with or violation of the PDPA may result in the following penalties and liabilities: **Civil Liability:** If a violation causes damage to a data subject, the data controller or data processor must compensate the injured data subject for the actual damages. In certain cases, the court may also award punitive damages up to twice the amount of actual damages. **Administrative Penalties:** Administrative fines range from not exceeding THB 1 million (approx. USD 33,333) to not exceeding THB 5 million (approx. USD 166,667), depending on the nature and severity of the offence. The Expert Committee, designated by the PDPC, has the authority to impose administrative penalties. For non-severe offences, the Expert Committee may issue other administrative measures such as a warning, an order to rectify, or an order to suspend the processing activity. If the offence is considered severe, or if the offender fails to comply with an administrative order, the Expert Committee may then impose an administrative fine. **Criminal Penalties:** The use, disclosure, or transfer of sensitive personal data in violation of the PDPA with malicious intent, for example, in a manner that is likely to cause another person to suffer any damage, impair his or her reputation, or expose such other person to be scorned, hated, or humiliated, etc.), may result in imprisonment for a term not exceeding 6 months to not exceeding 1 year and/or fine not exceeding THB 500,000 (approx. USD 16,667) to not exceeding THB 1 million (approx. USD 33,333). In addition, any person who gains access to another person's personal data in the course of their duties under the PDPA and unlawfully discloses such data is subject to criminal penalties of imprisonment for a term not exceeding 6 months and/or fine not exceeding THB 500,000 (approx. USD 16,667), unless the disclosure falls under the exemption.

For criminal offences, if the act results from the action or omission of a company's director, manager, or responsible person, that individual may also be held liable to the same criminal penalties.

Do data subjects have any private remedies?	**Yes.** Aggrieved individuals have the right to bring a civil action against the data controller or data processor to claim compensation for actual damages, as detailed in Civil Liability above.
Has the data privacy regulator issued any notable enforcement guidance or judgments in the last 12-24 months?	**Yes.** We note that the PDPC has become very active recently, and the PDPC has announced to the press on 1 August 2025 (here) that it had issued eight new administrative fines under the PDPA in five cases of noncompliance by public and private entities. The enforcement actions reflect a growing commitment by the PDPC to penalize noncompliance across all sectors, regardless of organizational type or size. The total amount imposed to date was approximately THB 21.5 million (approx. USD 654,690), underscoring the financial risks tied to PDPA violations.

Associated Contacts

Charmian Aw

Singapore

Email Me

Ciara O'Leary

Singapore

Email Me

Vietnam

Last updated 16 September 2025

Overview of Personal Data Protection Laws

What is the principal legislation, law or regulation	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

governing personal data protection?

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.

Definitions

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 provide to them?	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.

Legal Bases for 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

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	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.

information required to be covered?

Minors' Data

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

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.

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 Marketing, Online Tracking and Cookies

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

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

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	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 similar online tracking tools?	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 tracking tools?	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.

Data Sharing and Processor Obligations

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.

Cross-Border Transfers

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 Requirements

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	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.

requirements?

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

Are there obligations to register with or notify the data protection authority in order to collect or process personal data generally?	Yes. a. **What are these obligations and their timing requirements?** 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 and Breach Notification

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

from unauthorized access?	
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.

Regulatory Authority and Enforcement

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.
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

Charmian Aw

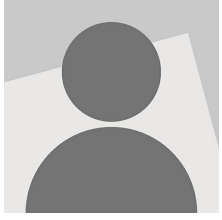
Singapore

Email Me

Gaston Fernandez

Hanoi, Ho Chi Minh City

Email Me



Duong Pham

Hanoi

Email Me

Hanh VU

Email Me

Disclaimer