

DATA PROTECTION LAWS OF THE WORLD

Brunei



Downloaded: 11 May 2024

BRUNEI



Last modified 3 January 2024

LAW

At present there are no statutory or common law obligations that protects the privacy of information upon which an individual can be directly or indirectly identified, save in respect of banker – customer relationship where banks are under a legal duty to keep customer information confidential.

However, with the publication of the Public Consultation Paper on Personal Data Protection for the Private Sector in Brunei Darussalam by the Authority for Info-communications Technology Industry of Brunei Darussalam (**AITI**) on 20 May 2021 and the Response to Feedback on Public Consultation Paper on Personal Data Protection for the Private Sector published on 3 December 2021 (together, the **Public Consultation Paper**), it is anticipated that the Personal Data Protection Order (**PDPO**) will be enacted and come into force in the near future. Premise on the Public Consultation Paper, which sets out in general terms the data protection framework under the PDPO, it is anticipated that the PDPO will introduce obligations on the part of private sector organizations with respect to collection, use, disclosure or other processing of individuals' personal data and the rights of individuals in relation to the processing of their personal data.

DEFINITIONS

Definition of personal data

At present there is no legal definition.

It is anticipated that under the PDPO "personal data" will refer to data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organization has or is likely to have access. Premised on such a definition of “personal data” it is envisaged that if a data subject cannot be identified by that data and other information to which the organization has or may have access to, such data would not come within the meaning of “personal data” under PDPO and this would remain the situation regardless of any anonymisation technique having been applied to the data. Noting that there are complexities surrounding the concept of anonymisation, AITI have expressed their intentions to provide guidance on anonymisation in due course.

Definition of sensitive personal data

At present there is no legal definition.

It is anticipated that the PDPO will not make a distinction between sensitive and non-sensitive personal data or define a category of “sensitive personal data”.

NATIONAL DATA PROTECTION AUTHORITY

At present nil.

It is anticipated that the PDPO will establish a national data protection authority referred to as the Responsible Authority. It is anticipated that AITI will be designated as the Responsible Authority.

REGISTRATION

At present no legal requirement.

It is anticipated that the PDPO will not have any registration requirements.

DATA PROTECTION OFFICERS

At present no legal requirement.

It is anticipated that the PDPO will require an organization to appoint a data protection officer who shall be responsible for ensuring that the organization complies with the PDPO and develops and implement policies and practices that are necessary to meet its obligations under the PDPO including a process to receive complaints. AITI have expressed the possibility of them issuing advisory guidelines to provide clarity and guidance on the topic of Data Protection Officers in the future.

COLLECTION & PROCESSING

At present not a regulated activity.

Under the PDPO framework set out in the Public Consultation Paper, organizations may collect, use or disclose personal data about an individual for purposes that a reasonable person would consider appropriate in the circumstance.

It is anticipated that under the PDPO organizations may collect, use or disclose personal data where:

- they have the prior consent of the individual;
- unless otherwise required or authorized by law; or
- an exception in the PDPO applies.

Where consent is required, it is anticipated that the PDPO will not specifically prescribe the manner in which consent may be given and that the PDPO will recognize that consent may be explicit or implicit through an individual's actions or inactions, depending on the circumstances, and thereby allowing organizations flexibility as to how they obtain consent. That said, it is anticipated that the PDPO would require organizations to look to express consent as the first port of call and only rely on deemed consent or the exceptions to consent if obtaining consent is impractical or if they have otherwise failed to obtain express consent.

It is anticipated that under the PDPO consent must be validly obtained and consent would not be valid where:

- consent is obtained as a condition of providing a product or service and such consent is beyond what is reasonable to provide the product or service to the individual; the principle being that organizations should not collect more personal data than is reasonable and necessary; and
- where false or misleading information was provided in order to obtain or attempt to obtain the individual's consent for collecting, using or disclosing his personal data.

As part of obtaining valid consent, it is anticipated that the PDPO will require organizations to provide the individual with information on:

- the purposes for the collection, use or disclosure of his personal data, on or before collecting the personal data; and
- any other purpose for the use or disclosure of personal data that has not been notified to the individual, before such use or disclosure of personal data.

Further, it is anticipated that fresh consent would be required where personal data collected is to be used for a different purpose from which the individual originally consented.

For a minor (a person below the age of 18 years) who is unable to give consent to an organisation to collect, use and disclose his personal data, the organisation will have to obtain consent from a parent or legal guardian of the minor. AITI have expressed their intentions to provide guidance on data processing activities relating to minors in the future.

TRANSFER

At present not a regulated activity.

It is anticipated that under the PDPO, an organization shall not transfer personal data to a country outside Brunei Darussalam except in accordance with requirements prescribed under the PDPO to ensure that the transferred personal data will be accorded a standard of protection that is comparable to that under the PDPO. It is not anticipated that such requirement prescribed by the PDPO will be as stringent and prescriptive as in other jurisdiction, for example the EU, and it is anticipated that the PDPO will place the onus on organizations to ensure that appropriate measures are taken to protect personal data transferred out of Brunei Darussalam through the imposition of contractual obligations or otherwise.

AITI recommends the adoption of the ASEAN Model Contractual Clauses for Cross Border Data Flows (**MCCs**) which are templates for contractual terms and conditions which may be included in legal agreements between businesses to ensure personal data is protected when engaging in cross border data transfers between ASEAN Member States. But it remains to be seen if the adoption of the MCCs will be popular as it is envisaged that a fair amount of modification will have to be made to the MCCs so as to be compatible with the purposes of any particular cross-border transaction between organisations.

SECURITY

At present not a regulated activity save in relation to a "Financial Institution" — see [Mandatory Breach Notification](#).

It is anticipated that under the PDPO, an organization must protect personal data in its possession or under its control by making reasonable security arrangements to prevent:

- unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks; and
- the loss of any storage medium or device on which personal data is stored.

It is anticipated that under the PDPO data intermediaries will also be subjected to the same obligation to protect personal data in their possession.

It is anticipated that the PDPO will provide for a reasonable standard for such security measures taking into account factors such as the nature and sensitivity of the data, the form in which personal data is stored and the impact to the individual if the personal data is subject to unauthorized access, disclosure or other risks. But it is not anticipated that the PDPO will stipulate specific security measures to be adopted and implement by organizations and data intermediaries. That said, AITI have expressed their intentions to issue detailed guidance on the types of security measures, which will include administrative / organisational, physical and technical security measures in due course.

BREACH NOTIFICATION

Mandatory Breach Notification

At present no legal requirement save in relation to a "Financial Institution" (i.e. banks, insurance companies, moneylenders, pawnbrokers, moneychangers and securities service providers licensed in Brunei Darussalam).

It is anticipated that under the PDPO, organizations are required to, as soon as practicable, but in any case no later than 3 calendar days after the assessment, notify the Responsible Authority of a data breach that:

- results in, or is likely to result in, significant harm to the individuals to whom any personal data affected by a data breach relates; or
- is or is likely to be, of a significant scale.

AIIT have expressed their intentions to issue guidelines on “significant harm”; and “significant scale”; in the near future.

Organizations are also anticipated to be required to notify the affected individuals on or after notifying the Responsible Authority if the data breach results in, or is likely to result in, significant harm to an affected individual.

Further, it is anticipated that unreasonable delays in reporting breaches that cannot be justified will be considered a breach of the data breach notification obligation.

Where a data breach is discovered by a data intermediary, it is anticipated that under the PDPO, the data intermediary will be under a duty to notify the organization or the Responsible Authority of the data breach.

A Financial Institution is obliged to report to the Brunei Darussalam Central Bank, no later than 2 hours after confirmation of all instances of cyber intrusion, disruption, malfunction, error or cybersecurity issues on a Financial Institution's system, server, network or end-point which has a severe or widespread impact on the operations and service delivery or has a material impact on the Financial Institution.

ENFORCEMENT

At present no enforcement authority.

It is anticipated that under the PDPO the Responsible Authority will administer and enforce the PDPO and will have the powers to do any of the following:

- issue directions to organizations to:
 - stop collecting, using or disclosing personal data in contravention of the PDPO;
 - destroy personal data collected in contravention of the PDPO; or
 - provide access to or correct personal data.
- impose a financial penalty of up to BND1 million or 10% of the annual turnover of an organization for negligent or intentional breach of the PDPO.

ELECTRONIC MARKETING

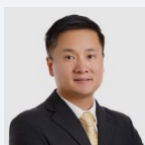
No legal requirement to have privacy policies.

ONLINE PRIVACY

No legal requirement to have privacy policies.

KEY CONTACTS

Abraham, Davidson & CO.
www.adcobrunei.com/



Linus Tan
Partner
Abraham, Davidson & CO.
T +673 2242840
linus_tan@adcobrunei.com



Elaiza Hanum Merican
Associate
Abraham, Davidson & CO.
T +673 2242840
elaiza@adcobrunei.com

DATA PRIVACY TOOL

You may also be interested in our [Data Privacy Scorebox](#) to assess your organization's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.