March 2022

Quick Legal Tips – from Bird & Bird

KNOWING ABOUT DATA PROTECTION FOR YOUR COMPANY

Given the increasing digitalisation of businesses, there has been an increasing emphasis on personal data and data protection in today's context. The General Data Protection Regulation, or in short, the GDPR, will sound familiar to many and particularly, the high-profile court cases involving Max Schrems and Facebook over the years.

Locally, the Personal Data Protection Act 2012 ("**PDPA**") is the governing data protection legislation in Singapore. Although the PDPA is neither as comprehensive nor as stringent as the GDPR, recent amendments have appeared to bring the PDPA to be more in line with the GDPR.

For the purposes of this article, the focus will be on the data protection obligations imposed on companies by the PDPA.

A. What is Personal Data?

Personal data is defined in the PDPA as "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 organisation has or is likely to have access.

An "individual" is also defined in the PDPA to refer to a natural person, whether living or deceased.

Examples of personal data will include an individual's residential address, NRIC, health, educational, as well as his employment background. Business contact information (such as an individual's business email address, business telephone number, position name or title) does not constitute as personal data.

B. Scope of the PDPA

The data protection provisions of the PDPA generally applies to organisations. Organisations are defined in the PDPA to include individuals, companies, associations, or bodies of persons, corporate or unincorporated.

The definition of organisations in the PDPA include organisations that are (i) formed or recognised under the law of Singapore; or (ii) resident, or having an office or a place of business, in Singapore. This would necessarily include foreign entities and individuals.

In terms of material scope, the PDPA governs the collection, use, and disclosure of an individual's personal data by organisations. The PDPA imposes obligations on organisations to protect personal data in its possession or under its control and requires organisations to ensure that its relevant computer systems are secured.

C. Data Protection Obligations

The PDPA sets out 10 overriding obligations in accordance with which all personal data must be obtained, used and disclosed. Each of these obligations is identified below:

(i) The Consent Obligation

The PDPA prohibits organisations from collecting, using or disclosing an individual's personal data unless consent or deemed consent was obtained from the individual. Consent must be freely given, specific and informed.

An individual has not given consent unless the individual has been notified of the purposes for which his personal data will be collected, used and disclosed, and that individual has provided consent for those purposes.

Although verbal consent is permissible, it is recommended that consent be obtained in writing or recorded in a manner that is accessible for future reference.

There are 3 situations in which deemed consent may be obtained:

(a) Deemed consent by conduct: This applies in situations where the individual voluntarily provides his personal data to the organisation.

(b) Deemed consent by contractual necessity: This applies in situations where the individual provides his personal data to one organisation ("**A**") for the purpose of a transaction and it is reasonably necessary for A to disclose the personal data to another organisation ("**B**") or a further downstream organisation ("**C**") for the necessary conclusion or performance of the transaction between the individual and A.

(c) Deemed consent by notification: This applies in situations where the individual can be said to have consented to the collection, use or disclosure of personal data for a purpose that he/she had been notified of, and he has not taken any action to opt out of the collection, use or disclosure of his personal data. Note that organisations must provide a reasonable period for the individual to opt out before it proceeds to collect, use or disclose the personal data.

Consent cannot be a condition of providing any product or service.

Consent may be withdrawn at any time by an individual, and an organisation must allow and facilitate the withdrawal of consent.

(ii) The Purpose Limitation Obligation

An organisation may collect, use or disclose personal data about an individual only for the purposes that a reasonable person would consider appropriate in the circumstances, and where applicable, that the individual has been informed of the purposes.

(iii) The Notification Obligation

All organisations are required to notify individuals of the purposes for which their personal data is being collected, used and disclosed on or before such collection, use or disclosure.

(iv) The Access and Control Obligations

All organisations are required to notify the individuals that they are entitled to request for access to, and correction of, their personal data. The organisations are further required to respond to all

such access or correction requests as soon as reasonably possible or as soon as practicable from the time the access or correction requests were received.

The exceptions to the obligation to allow access to personal data are as follows:

- The opinion data was kept solely for an evaluative purpose.
- The data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation
- The requests would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the request.
- If the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests.
- The request could reasonably be expected to threaten the safety or physical or mental health of an individual other than the individual who made the request.
- The request could reasonably be expected to cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request.
- The request could reasonably be expected to reveal personal data about another individual.

There are also exceptions to the obligation to correct personal data, e.g. where the opinion data is kept solely for evaluative purposes, or data is part of a professional / expert opinion.

Organisations may charge an individual a reasonable fee for access to personal data about the individual. However, no fees can be charged for the correction of personal data.

(v) The Accuracy Obligation

Organisations are required to make a reasonable effort to ensure that personal data so collected is accurate and complete, if the personal data is likely to be to make a decision that affects the individual to whom the personal data relates; or to be disclosed to another organisation.

(vi) The Protection Obligation

Organisations are required to implement reasonable security arrangements to protect the personal data under their possession or control to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Reasonable security arrangements are also required to be implements to prevent the loss of any storage medium or device on which personal data is stored.

(vii) The Retention Limitation Obligation

Organisation are required to cease retaining documents that contain personal data, and remove the means by which the personal data can be associated with any particular individuals, as soon as it is reasonable to assume that the purpose(s) for which that personal data was collected is no longer being served by retention of the personal data, and retention is no longer necessary for legal or business purposes.

(viii) The Transfer Limitation Obligation

Organisations are generally not permitted to transfer personal data outside of Singapore unless that organisation has taken appropriate steps to ensure that the overseas recipient is bound by

legally enforceable obligations or specified certifications to provide the transferred personal data a standard of protection that is comparable to that under the PDPA.

Examples of legally enforceable obligations include contracts or binding corporate rules that imposes a standard of protection that is comparable to that under the PDPA. These contracts or binding corporate rules should also, for instance, specify the countries and territories to which the personal data may be transferred under the contract.

If organisations are unable to rely on legally enforceable obligations or specified certifications, the following circumstances should be adhered to:

- the individual whose personal data is to be transferred gives his consent to the transfer of his personal data after being provided with a reasonable summary in writing of the extent to which the transferred personal data will be protected;
- the individual is deemed to have consented to the disclosure by the transferring organisation of the individual's personal data where the transfer is reasonably necessary for the conclusion or performance of a contract between the organisation and the individual, including the transfer to a third party organisation;
- the transfer is necessary for a use or disclosure that is in the vital interests of individuals or in the national interest, and the transferring organisation has taken reasonable steps to ensure that the personal data will not be used or disclosed by the recipient for any other purpose; and
- the personal data involved is data in transit / publicly available in Singapore.

(ix) <u>The Data Breach Notification Obligation</u>

The PDPA imposes a duty on organisations to assess whether a data breach is notifiable, and to notify the affected individuals and/or the PDPC Commission where it is assessed to be notifiable.

To assess whether a data breach is notifiable, two factors are considered:

(a) Whether there is significant harm to affected individuals; and
(b) Whether the data breach is of a significant scale.

On (a), examples of personal data (or classes of personal data) that is deemed to result in significant harm to affected individuals are as follows:

- Individual's full name or alias or full national identification number in combination with any of the following personal data below:
    - Financial information which is not publicly disclosed.
    - Identification of vulnerable individual.
    - Life, accident and health insurance information which is not publicly disclosed.
    - Specified medical information.
    - Information related to adoption matters.
    - Private key used to authenticate or sign an electronic record or transaction.

On (b), data breaches that meet the criteria of significant scale are those that involve the personal data of 500 or more individuals. Where a data breach affects 500 or more individuals, the organisation is required to notify the PDPC Commission, even if the data breach does not involve any of the prescribed personal data above.

(x) The Accountability Obligation

Organisations are required to undertake measures to meet their obligations under the PDPA, including but not limited to:

- appointing a data protection officer to ensure that organisation's compliance with the PDPA;
- developing and implementing data protection policies and practices; and
- making information about their data protection policies and practices publicly available.

D. Employee Personal Data

Organisations should inform the employees of the purposes for the collection, use and disclosure of their personal data and obtain their consent prior to the collection, use and disclosure.

The PDPA does not specify the form or manner that organisations are required to use which would provide their employees with the required information about the purposes for which the employees' personal data would be collected, used and disclosed by the organisations. As such, the organisations have the discretion to determine the appropriate form on notification to their employees of the purposes, e.g. through employment contracts, employee handbooks, or notices in the intranet. In most cases, consent is obtained at the point of appointing the new employee and at various points during the employment relationship when the organisation requires more personal data or intends to use or disclose the employee's personal data for other purposes. Even if consent is given, employees may withdraw that consent under the PDPA.

Organisations may however collect, use and disclose personal data of their employees without consent where it is reasonable for the purpose of or in relation to the organisation:

(a) entering into an employment relationship with the individual or appointing the individual to any office; or
(b) managing or terminating the employment relationship with or appointment of the individual.

Please note that while consent is not required, employers are nevertheless still required to notify their employees of the purposes of such collection, use or disclosure.

Where an individual voluntarily provides his personal data to an organisation in the form of a job application, he may be deemed to consent to the organisation collecting, using and disclosing the personal data for the purpose of assessing his job application. If the individual is subsequently employed, it would be reasonable for the organisation to continue to use the personal data provided by the individual. If the organisation wishes to use the personal data for purposes for which consent may not be deemed or to which there is no applicable exception under the PDPA, the organisation must then inform the individual of those purposes and obtain his consent, unless relevant exceptions apply.

Sandra Seah
Joint Managing Partner
Sandra.seah@twobirds.com
Direct +65 6428 9429

Terrance Goh
Associate
terrance.goh@twobirds.com
Direct +65 6428 9805