DREW & NAPIER

LEGAL UPDATE

LEGAL UPDATE
24 May 2019

PDPC ISSUES DATA PORTABILITY PUBLIC CONSULTATION PAPER AND GUIDES ON ENFORCEMENT AND DATA BREACH MANAGEMENT

INTRODUCTION

On 22 May 2019, the Personal Data Protection Commission ("**PDPC**") issued a Public Consultation on Data Portability and Data Innovation Provisions ("**Public Consultation**"), as part of its review of the Personal Data Protection Act (No. 26 of 2012) ("**PDPA**"). In addition, the PDPC also issued a Guide on Active Enforcement ("**Active Enforcement Guide**"), revamped its Guide to Managing Data Breaches 2.0 ("**Data Breach Guide 2.0**"), and revised its earlier Guide to Developing a Data Protection Management Programme ("**DP Management Programme Guide**").

PUBLIC CONSULTATION PAPER ON DATA PORTABILITY AND DATA INNOVATION PROVISIONS

The Public Consultation seeks feedback and input from relevant stakeholders and interested parties on two broad areas:

(a) the PDPC is proposing to introduce data portability provisions under the PDPA, which aim to give individuals greater control over their personal data by allowing them to request their data held by an organisation to be transmitted to another organisation in a commonly used machine-readable format. This will enable individuals to move their data across services and enable greater access to more data by organisations; and

(b) the PDPC is proposing to introduce data innovation provisions under the PDPA, which complement the data portability provisions by making it clear that organisations can use data for appropriate business purposes.

The Public Consultation can be accessed here.

We set out below a non-exhaustive summary of the Public Consultation as well as the list of issues that the PDPC has sought feedback on.

Data portability

The PDPC is considering the introduction of a Data Portability Obligation under the PDPA, which would require organisations, at the request of individuals, to transmit an individual's data that is in the organisation's possession or under its control to another organisation in a commonly used machine-readable format ("**data porting request**").

As data portability is intended to support the digital economy, the Data Portability Obligation will only apply to data in the possession or control of organisations that is held in electronic form, regardless of whether it was originally collected in electronic or non-electronic form.

Crucially, the data that will be covered by the Data Portability Obligation is not limited to personal data as defined under the PDPA. The data covered by the Data Portability Obligation includes data that is provided by individuals to the organisation, or generated by individuals' activities in using the organisation's products or services. However,

organisations will not be obliged to reveal confidential commercial information that could harm their competitive position, or data that is derived from their own business-specific internal processing of data.

The Data Portability Obligation will apply to any organisation that collects, uses or discloses personal data in Singapore, except for the following:

(a) any individual acting in a personal or domestic capacity;
(b) any employee acting in the course of his or her employment with an organisation;
(c) any public agency; and
(d) any organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of personal data.

Any individual, whether or not in Singapore, may make a data porting request, although organisations will only be required to transmit data to other organisations that have a presence in Singapore. Nonetheless, organisations may voluntarily transmit data to overseas organisations with the consent of the individuals concerned.

In handling a data porting request, organisations will have the following key responsibilities:

(a) Receiving the request – providing an avenue for individuals to make a data porting request.
(b) Verifying the request – ensuring the veracity of the request by, for example, requiring a secure online login.
(c) Verifying the data to be ported – allowing individuals to view the data, or a sample thereof, to ascertain which data the individuals wish to be ported.
(d) Porting the data – providing individuals with information on the fees chargeable, where reasonable to cover the costs of porting, and when the data will be ported to the receiving organisation(s).
(e) Formatting the data to be ported – ensuring that data ported is in an easily accessible and affordable format, ideally an open data format.
(f) Informing individuals of a rejection – informing individuals of reasons for rejecting a data porting request (e.g., organisation does not hold data that is covered by the Data Portability Obligation).
(g) Preserving the data – preserving a copy of data ported, for at least 30 calendar days after rejecting a request.
(h) Withdrawal of request – ceasing the process of transmitting the data should the requesting individuals withdraw the request to data.

Insofar as the ported data contains personal data, organisations receiving ported data will be treated as collecting personal data and the Data Protection Obligations under the PDPA will apply.

The Data Portability Obligation will not apply to data intermediaries in relation to data that it is processing on behalf of and for the purposes of another organisation, but organisations may engage data intermediaries to respond to data porting requests on its behalf.

To enforce the Data Portability Obligation, the PDPC will have powers to review an organisation's:

(a) refusal to port data;
(b) failure to port data within a reasonable time; and
(c) fees for porting data.

The PDPC will also issue relevant binding codes of practice in due course governing among others, consumer safeguards, counterparty assurance, interoperability, and security of data.

Data innovation

To enable organisations to confidently use data to derive business insights and innovate in the development and delivery of products and services, the PDPC intends to introduce provisions in the PDPA to clarify that organisations can use personal data, collected in compliance with the PDPA, for the business innovation purposes of:

(a) operational efficiency and service improvements;
(b) product and service development; or
(c) knowing customers better.

Organisations may use, but not collect or disclose, personal data for business innovation purposes, without having to comply with the Notification and Consent Obligations. Even where individuals have withdrawn their consent for the use or disclosure of personal data for the original purposes for which the data was collected, organisations may continue to use such personal data for business innovation purposes. However, the PDPC has made it clear that this will not extend to the use of

data for sending direct marketing messages to customers without their consent.

In relation to the Retention Limitation Obligation, the PDPC intends to clarify that the business innovation purposes will be considered business purposes for which retention of the personal data may be necessary. This will permit organisations to retain personal data even where the individual has withdrawn consent for the original purposes of the collection, use or disclosure of his or her personal data.

The PDPC also proposes to include in the PDPA a concept of "derived personal data", created through the processing of other data by applying business-specific internal processing. The Data Protection Obligations will generally apply to derived personal data, especially the Accuracy Obligation, where organisations are required to make reasonable efforts to ensure the accuracy and completeness of personal data that is used by the organisation to make decisions regarding particular individuals or which is likely to be disclosed to another organisation.

The PDPC proposes to provide that derived personal data will not be subject to the Access, Correction, and Data Portability Obligations. Organisations will therefore not be required to accede to requests to correct the derived personal data. But where individuals make a request to correct an error or omission in the underlying personal data processed to create derived personal data, organisations are required to make that correction, which may extend to any personal data used to create the derived data so as to ensure the accuracy of the data held by the organisation. Organisations will also be required to provide individuals with information about the ways in which the derived personal data has been or may have been used or disclosed by the organisation within a year before the date of request.

Issues raised

In summary, the PDPC has sought public feedback on the following:

(a) the impact of data portability, specifically on consumers, the market, and the economy;
(b) the scope of organisations and data covered by the Data Portability Obligation;
(c) the proposed exceptions to the Data Portability Obligation;
(d) the proposed requirements for handling data portability requests;
(e) the proposed powers for the PDPC to review an organisation's refusal to port data, failure to port data within a reasonable time, and fees for porting data;
(f) the proposed binding codes of practice that set out specific requirements and standards for the porting of data in specific clusters or sectors;
(g) the proposed approach for organisations to use personal data for the specified business innovation purposes without the requirement to notify and seek consent to use the personal data for such purposes;
(h) the proposed definition of "derived data"; and
(i) the proposal for the Access, Correction, and proposed Data Portability Obligations to not apply to derived personal data.

Stakeholders and interested parties are invited to provide their feedback to the PDPC by email to corporate@pdpc.gov.sg by 5pm on 3 July 2019.

GUIDE ON ACTIVE ENFORCEMENT

The Active Enforcement Guide outlines the PDPC's enforcement framework and policies, covering its investigation process, types of enforcement actions, and financial penalties imposable under the PDPA. The PDPC aims to deploy its enforcement powers to act effectively and efficiently on an increasing number of data-related incidents.

The Active Enforcement Guide can be accessed here.

Types of enforcement actions

We highlight in particular, the various enforcement actions that the PDPC may take against organisations that are investigated:

(a) suspension or discontinuation of the investigation;
(b) undertaking;
(c) expedited decision; and
(d) full investigation process, which may result in a finding of no breach, a warning, directions, financial penalties, or directions and financial penalties.

Suspension or discontinuation

The Active Enforcement Guide clarifies that the PDPC may choose to suspend or discontinue investigations where it assesses the data protection impact of a case to be low. Such situations may include where the parties have reached a mutual agreement to settle the matter, where the complainant has commenced private legal proceedings in respect of alleged contraventions of the PDPA, or where the PDPC considers that a complaint is frivolous or vexatious or is not made in good faith.

When the PDPC chooses to suspend or discontinue investigations, the PDPC will also issue an advisory notice to organisations involved. Such an advisory notice is not a finding of breach but serves as a tool of instruction highlighting the areas that the organisations can improve on so as to be compliant with the PDPA.

Undertaking

The undertaking process is intended to allow organisations with good accountability practices and drawer plans (e.g., data management and incident response plans) to implement such plans and demonstrate their commitment to compliance with the PDPA. Such plans must be implemented shortly after the breach occurs, and organisations will not be given additional time to produce such plans.

The undertaking process may be initiated by the PDPC or the organisation, where the organisation voluntarily commits to remedy the breaches and to take steps to prevent any recurrences. However, the PDPC reserves the right not to accept undertaking requests such as where organisations do not demonstrate good accountability practices, refuse to accept the undertaking terms and conditions, seek to impose terms and conditions on the PDPC beyond those relating to confidentiality of information, or do not agree for the undertaking to be published.

Expedited Decision

Where there is an upfront admission of liability by the organisation involved on its role in the cause of the breach that is of a similar nature to precedent cases, organisations may make a written request to the PDPC to consider issuing an expedited decision at the commencement of investigations.

Expedited decisions are intended to reduce the time and resources required for investigations significantly, partly through the voluntary admission of the relevant facts and the organisation's role in a breach. However, the PDPC will still issue a full decision even if it is expedited, which will set out the relevant direction(s), including any financial penalties.

Full investigation process

The PDPC will launch the full investigation process when it considers that incidents with high impact have occurred, such as when a large number of individuals are affected and where the personal data disclosed could cause significant harm. The length of the full investigation process will depend on the level of cooperation from the organisations involved but the PDPC estimates that it generally takes between 6 to 18 months.

Financial penalties

As a matter of enforcement policy, the PDPC will consider the nature of the breach and whether directions without financial penalties are effective in remedying the breach. Financial penalties are intended to act as a form of sanction and deterrence against non-compliance when directions alone do not sufficiently reflect the seriousness of the breach.

The Active Enforcement Guide sets out the factors that the PDPC will consider in assessing the seriousness of the breach, and in determining the quantum of the financial penalty to be imposed.

GUIDE TO MANAGING DATA BREACHES 2.0

In view of the PDPC intending to introduce a mandatory data breach notification requirement under the PDPA, the Data Breach Guide has been revised from its previous version issued in 2015. The Data Breach Guide covers how organisations should generally prepare for data breaches, as well as how organisations should respond to data breaches.

The Data Breach Guide can be accessed here.

Preparing for data breaches

In preparing for data breaches, organisations should put in place monitoring measures as well as a data breach management plan.

In particular, a data breach management plan helps organisations manage and respond to data breaches more effectively, and should set out the following:

(a) a clear explanation of what constitutes a data breach, both suspected and confirmed;
(b) how to report a data breach internally;
(c) how to respond to a data breach, including designating a data breach management team; and
(d) the responsibilities of the data breach management team.

In this regard, the PDPC has also revised and issued the DP Management Programme Guide, which can be accessed here.

Responding to data breaches

The Data Breach Guide also recommends that organisations take the following four key steps in responding to a data breach:

(a) contain the data breach to prevent further compromise of personal data;
(b) assess the data breach by gathering facts and evaluating risks, including the harm to affected individuals;
(c) report the data breach to PDPC and/or affected individuals, as necessary; and
(d) evaluate the organisation's response to the data breach incident and consider the actions which can be taken to prevent future data breaches.

First, to contain data breaches, organisations should act swiftly. An initial assessment of the data breach should be conducted to determine the severity of the data breach, in order to decide on the immediate actions that need to be taken, as well as to allow the organisation to better inform any external assisting parties. The initial assessment should include the following:

(a) the cause of the data breach and whether the breach is still ongoing;
(b) the number of affected individuals;
(c) the types of personal data involved;
(d) the affected systems and/or services; and
(e) whether help is required to contain the breach.

Organisations should also consider notifying the Police as well as the Cyber Security Agency of Singapore if they suspect that criminal acts have been perpetrated. In addition, organisations are advised to be mindful of any sectoral regulations that may apply for data breaches.

Second, to assess a data breach, the organisation should consider the context of the data breach (e.g., sensitivity of personal data, profile of affected individuals, whether personal data was publicly available), the ease of identifying individuals from the compromised data, and the circumstances of the data breach. This is to allow organisations to conclude whether the data breach is unlikely or likely to result in significant impact or harm to the affected individuals, and to consider and take steps to reduce any such potential harm or impact as necessary.

Third, organisations are obliged to report to the PDPC and the affected individuals if the breach is assessed to be likely to result in significant harm or impact to the individuals to whom the personal data relates, or is of a significant scale. Organisations should assess the severity of a breach within 30 days, and notify the PDPC no later than 72 hours after establishing that the data breach is a notifiable breach; the affected individuals should be notified as soon as practicable although no definite timeframe is given.

Last, organisations should evaluate the effectiveness of its initial containment efforts and decide whether further remedial efforts are necessary. Organisations should review and learn from the data breach incident to improve their personal data handling practices and to prevent the reoccurrence of similar data breaches.

We will continue to monitor developments in this area, and provide you with relevant updates.

If you have any questions or comments on this article, please contact:

Lim Chong Kin
Director
Head, Telecommunications, Media and Technology
T: +65 6531 4110
E: chongkin.lim@drewnapier.com

Drew & Napier LLC
10 Collyer Quay
#10-01 Ocean Financial Centre
Singapore 049315

www.drewnapier.com

T : +65 6535 0733
T : +65 9726 0573 (After Hours)
F : +65 6535 4906