RECENT UPDATES TO THE PERSONAL DATA PROTECTION ACT INVESTIGATION AND ENFORCEMENT REGIME

Posted on May 28, 2019

Category: CNPupdates

Date Published: 28 May 2019

Authors and Contributors: Wong Pei Ling, Lorraine Liew, Stephen Soh and Susannah Dobbie.

The Guide on Active Enforcement and Guide to Managing Data Breaches 2.0 released by the Personal Data Protection Commission ("**PDPC**") on 22 May 2019 (collectively, the "**Guides**") are the latest in a series of guides published by the regulatory body to assist organisations in understanding the PDPC's approach to regulating Singapore's personal data protection regime.

Almost five years on from the coming into force of the main data protection provisions of the Personal Data Protection Act ("**PDPA**") in July 2014, the PDPC has exercised its investigative and enforcement powers in respect of PDPA breaches of varying severity and has publicly released over 70 Grounds of Decisions (and other case summary digests) covering its findings.

Enforcement process

The enforcement process begins with a complaint or self-notification to the PDPC of a data breach incident, following which the PDPC will decide whether or not to investigate the matter. If the PDPC decides to investigate, it will engage in a fact-finding process through a variety of means, such as issuing notices to produce relevant documents and information, conducting interviews and making site visits. The Grounds of Decision sets out the PDPC's decision on whether or not there was a breach, and if so, what enforcement action it will take, which may include issuing a warning *only*, or directions (usually to undertake remedial

steps to improve the relevant organisation's data protection systems) and/or imposing financial penalties (up to S$1 million per breach).

The Guide on Active Enforcement provides an overview of and further insight into the various paths that an investigation may take and subsequent enforcement procedures. When considering whether to take enforcement actions, the PDPC is guided by the following key objectives:

1. to respond effectively to breaches of the PDPA where large groups of individuals are affected (for example exceeding 500 in number), and where such data breach is likely to cause harm or loss to the affected individuals;
2. to be proportionate and consistent in the application of enforcement action;
3. to ensure that organisations in breach take proper steps to correct gaps in the protection of personal data.

Specifically, the Guide on Active Enforcement sets out estimated timeframes for investigations and enforcement actions conducted by the PDPC in respect of an actual or suspected breach of the PDPA, some of which include:

Enforcement Actions	Summary/ Criteria	Estimated Timeline for Investigation Closure
Suspension or discontinuation of the investigation	The PDPC has the discretion to suspend, discontinue or decline to conduct investigations, and may do so where the impact of the breach incident is low, where the parties have mutually agreed to settle the matter, a party has commenced legal proceedings against the party in breach, the PDPC determines the matter is more appropriately investigated by another regulatory authority, or the complaint is frivolous or vexatious. An advisory notice, which is not a finding of breach, will be issued to the affected organisation.	3 months
Undertaking	May be initiated by either the PDPC and/or the affected organisation (subject to PDPC's discretion whether or not to accept the request). The request must be made either upon commencement or in the early stages of investigation. This process is intended for organisations which already have "drawer plans" for remediation and incident responses, ie. the incidents are foreseeable and the organisation has good accountability practices which it then undertakes to the PDPC in writing to forthwith implement and commits to remedy the breaches. The undertaking process will not be available in incidents when, inter alia, the organisation refuses responsibility for the data breach incident, requests time to produce a remediation plan, seeks to impose terms and conditions on the PDPC or refuses to accept the terms and conditions of the undertaking and refuses to publish the undertaking. The undertaking will be published in full, but the PDPC will consider redacting commercially confidential matters.	5 months
Expedited decision	The PDPC may make an expedited decision in response to a written request being made to the PDPC by the affected organisation providing an upfront admission of liability, at the commencement of an investigation (subject to the PDPC's discretion whether or not to accept the request). The organisation must be prepared to identify the obligations/areas to which it is admitting liability to and provide all relevant information. However, admissions might not be considered as a mitigating factor for repeated data breaches. The incident must be factually similar to precedent cases, some examples of which would include poor password policy, printing errors and poor IT governance A full decision will still be issued.	6 months
Full investigation process	A full decision will be issued at the conclusion of the investigation, which may result in the following decisions: • a determination that no breach occurred; • a determination that a breach occurred and a warning is issued; • providing directions; or imposing financial penalties; or • providing directions and imposing financial penalties.	18 months

It is

established that having good internal policies and processes assist in preventing data breaches from occurring, but the latest guidelines pertaining to investigations and enforcement mean that there is now an added incentive to take preparatory measures to anticipate a breach since it may make it easier for a well-prepared organisation to request an undertaking or expedited breach decision which have a considerably shorter estimated timeline (up to 5-6 months) instead of engaging in the full investigation process (up to 18 months).

Factors relevant to determining financial penalties

The Guide on Active Enforcement also sets out the factors that the PDPC considers in assessing the seriousness of a breach for the purposes of determining whether a financial penalty is appropriate and the financial penalty amount. Some of these factors include whether the organisation had acted deliberately or willfully, the number of individuals impacted, the type of personal data compromised and the extent of the organisation's non-compliance. The PDPC also aims to ensure that a financial penalty is proportionate to the seriousness of the breach and provides sufficient deterrence against future or continued non-compliance. The quantum may be affected by the presence of aggravating and mitigating factors, such as cooperativeness during the investigation, remedial measures are undertaken, voluntary notification and admission of liability.

Mandatory reporting of data breach incidents

Whilst the PDPC's enforcement actions have been primarily based on complaints or voluntary self-notification and the PDPA does not currently contain a mandatory obligation to notify the PDPC of a data breach, the PDPC has indicated its intention to introduce a mandatory data breach notification obligation into the PDPA in the near future.

The Guide to Managing Data Breaches 2.0, which amends the earlier guide issued in 2015, provides guidance on steps to take in reacting to a data breach incident. In particular, it outlines a process for notifying the PDPC and/or affected individuals when the data breach is likely to result in significant harm or impact to the affected individuals or the data breach is of a significant scale, meaning that the breach affects the personal data of 500 or more individuals. According to this process, the PDPC should be informed as soon as practicable, and no later than 72 hours after it is established that the data breach is one that is likely to result in significant harm or impact or is of a significant scale. Data intermediaries should inform their client of a potential or confirmed data breach within a period of no longer than 24 hours.

It is interesting to note that the Guide to Managing Data Breaches 2.0 sought to implement a timeline of no later than 72 hours after a data breach is established, which is consistent with the timeline prescribed for notification under the EU General Data Protection Regulation ("GDPR"), while the previous guide merely required that organisations notify the PDPC as soon as possible of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals. The PDPC appears to be

in the process of streamlining its data breach notification obligations in line with the notification requirements under the GDPR.

It is also pertinent to note that the Cybersecurity Act 2018, read with the Cybersecurity (Critical Information Infrastructure) Regulations 2018, make it mandatory for an owner of a computer system that is necessary for the continuous delivery of an essential service designated by the Commissioner of Cybersecurity as a critical information infrastructure ("**CII**") to notify the Commissioner of Cybersecurity of the occurrence of any prescribed cybersecurity incident in respect of the critical information infrastructure within 2 hours after becoming aware of the cyber security incident.

Conclusion

In light of the guidelines on the reporting of data breaches which are likely to become law, it is key for organisations to be able to react quickly to data breach incidents in assessing and evaluating the risks so that notification and remedial steps can be taken expeditiously. Organisations are highly encouraged to devise a data breach management plan using the guidelines provided in the Guides and the PDPC's Guide to Data Protection Management (revised version published on 22 May 2019). The Guide to Data Protection Management is useful in helping organisations identify data protection issues early, increase awareness of data protection across the organisation and identify risk points, and promotes awareness that a process or system has to be developed at the start, and not as an afterthought or response to data breaches.