

Client Alert

June 2019

For more information, please contact:

Ken Chia
+65 6434 2558
ken.chia@bakermckenzie.com

Anne Petterd
+65 6434 2573
anne.petterd@bakermckenzie.com

Alex Toh
+65 6434 2783
alex.toh@bakermckenzie.com

Daryl Seetoh
+65 6434 2257
daryl.seetoh@bakermckenzie.com

PDPC Guide on Active Enforcement Released

On 22 May 2019, the Personal Data Protection Commission (**PDPC**) published a Guide on Active Enforcement (**Guide**) that represents a change in the way that the PDPC handles enforcement actions going forward.

Under the current approach set out in the Advisory Guidelines on the Enforcement of the Data Protection Provisions (**Guidelines**), there are 3 main enforcement approaches. Where appropriate, PDPC could utilize alternative dispute resolution mechanisms, such as mediation and facilitated negotiations, to resolve what is perceived to primarily be a dispute between the parties. In the alternative, the PDPC could commence investigations that could involve the PDPC exercising the extent of its statutory powers of investigation under the Personal Data Protection Act (**PDPA**) to uncover facts and reach a decision. Lastly, where the organisation has made a decision involving the access and/or correction of personal data, the PDPC may review that decision.

The Guide sets out 2 other intermediate enforcement options - Voluntary undertakings and expedited decisions, that may be pursued in lieu of a full investigation. These were previously not expressly provided in the Guidelines or in the PDPA. The Guide provides information on the scope of these new options and the circumstances under which the PDPC will apply either enforcement option when investigating a breach.

This update is relevant to organisations who wish to better understand the new enforcement options that have become available and the preparatory steps that should be taken ahead of time to preserve the option for an organisation to seek an undertaking.

Undertaking

An undertaking is a written commitment by the organisation to the PDPC that voluntarily commits the organisation to remedy the breaches and take steps to prevent recurrence.

An undertaking is generally available when:

1. it achieves a similar or better enforcement outcome for the PDPC more effectively and efficiently than a full investigation; or
2. the organisation can show that it has accountable data privacy practices in place, or a Data Protection Trustmark (**Trustmark**), and that it has an effective remediation plan that it is prepared to implement. More information on the Trustmark can be found [here](#).

The remediation plan should include steps to reduce the recurrence of the incident as well as the implementation of monitoring and reporting processes, audits and policy/process reviews.



An undertaking will typically also include a description of the data breach incident and steps to notify and minimise harm to the affected individual(s). The PDPC also expects the organisation to have executive level endorsement to the undertaking - requiring that the undertaking be signed by the CEO or someone of equivalent rank.

The Guide also provides examples of the circumstances when the PDPC will not accept an undertaking request. For example, the PDPC will not accept an undertaking request when the organisation refutes responsibility for the data breach incident, refuses to accept the terms and conditions of the undertaking, or refuses to agree for the undertaking to be published. In particular, request for an undertaking must be made soon after investigations commence and the organisation must be ready with a remediation plan. The PDPC will not accept a request for an undertaking that requires for additional time to produce a remediation plan.

Of the 2 situations an undertaking is a viable option, the second option is partly within the control of the organisation that organisations can be prepared for. This requires organisations to be ready ahead of time to demonstrate good accountable privacy practices. Organisations that have done scenario planning and exercises to respond to data breach situations would be in a better position to prepare a remediation plan in the short time frame soon after investigations commence. Organisations who have taken the additional step to obtain a Trustmark certification are also put in a better position to seek an undertaking.

This underscores not only the importance of having documented processes in place but also organizational preparedness in managing potential data breach situations.

Expedited Decision

The PDPC may consider an expedited decision if there is an upfront admission of liability by the organisation(s) involved on its role in the cause of the breach. The organisation must submit a written request to the PDPC and must provide and admit to all facts relevant to the data breach incident. Generally, the PDPC will consider an expedited decision where the breach involves the failure to appoint a data protection officer or implement a privacy policy, or if the nature of the data breach is similar to precedent cases with similar categories of fact.

An expedited decision reduces the time frame for an investigation to be concluded. Although the PDPC will still issue a full decision (and the relevant directions), an admission of liability will be a strong mitigating factor if financial penalties are involved.



Full Investigation Process

The PDPC will usually launch a full investigation process immediately for data breach incidents with high impact, such as incidents where a large number of individuals are affected and the personal data disclosed could cause significant harm. Investigations that have been assessed to be of low impact may be discontinued.

If the PDPC determines that there has been a breach, the PDPC may impose: (i) a warning; (ii) directions only; (iii) financial penalties only; or (iv) directions and financial penalties.

You may find a copy of the Guide [here](#) and the Advisory Guidelines on the Enforcement of the Data Protection Provisions [here](#).

Please contact us should you have any further queries in relation to either.

©2019 Baker & McKenzie. All rights reserved. Baker & McKenzie International is a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

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