Hogan Lovells

From compliance to accountability: The changing face of data privacy in Singapore

5 August 2019

On 2 July 2014 the main provisions of the Personal Data Protection Act 2012 (PDPA) came into force. Five years on, what has Singapore learned about data privacy? A great deal, judging by the output and approach of the Personal Data Protection Commission (PDPC), not least the necessity to keep moving with these disruptive and fast-paced times.

A shift in emphasis

On 15 July 2019 the Commissioner of the PDPC noted that the explosion of personal data, along with the need to aggregate that data from a wide range of sources, has made the typical compliance-based approach to managing personal data increasingly impractical, unrealistic and damaging to innovation; "the approach of a box-checking exercise" would, Mr Tan Kiat How suggested, "overly constrain businesses in their use of data to create value and better service their customers". In an increasingly connected and competitive digital economy, organizations that focus on compliance may find themselves disadvantaged; "a simplistic and rigid approach would do more harm than good in the long term".

Indeed, as Singapore continues to ramp up its preparations for a future digital economy, the proliferation of artificial intelligence, machine learning, and the internet of things has challenged fundamental assumptions around the consent and notification requirements of handling personal data. In response, the PDPC will spearhead a shift in emphasis, from a compliance-based approach to an approach focused on "accountability".

The accountability game

To assist in this shift, the PDPC has released a *"Guide to Accountability"*. Accountability is, the guide suggests, "the undertaking and demonstration of responsibility for the personal data in the organization's possession or control". Specifically, accountability is divided into three broad areas:

1. Firstly, within an organization, by putting in place data privacy policies and practices;
2. Second, within the industry, by introducing measures to incentivise organizations; and
3. Finally, through enforcement procedures.

This shift from a compliance-based approach to an accountability-based approach will, it is hoped, strengthen trust with the public, enhance business competitiveness and ensure organizations are accountable in the three key areas of policy, people and process.

To break this down, "policy" is, as you would expect, an organization ensuring that data protection is embedded in its corporate governance, appointing data protection officers and communicating a clear approach to all stakeholders.

"People" emphasises that it is the responsibility of everyone in an organization to protect data, ensuring that practices are enforced top-down throughout an organization, with appropriate staff onboarding and training, and with easily-accessible policies.

Finally, "process" discusses the tools that can be used by an organization to document data flows, from collection to disposal, identifying key gaps and areas for improvement.

The practical effect of accountability

Whilst the PDPC has stated that the shift is "not a change in principle, but a shift in emphasis", this shift does have a number of important effects. For starters, the PDPA is now being amended. As well as introducing a mandatory breach notification requirement, the consent regime will be enhanced to ensure that organizations adopt accountable practices to better support responsible data innovation. The PDPC now recognizes "accountability" as one of the obligations of the PDPA, revising the current *"Openness Obligation"* to the *"Accountability Obligation"*, particularly in relation to Sections 11 and 12 of the PDPA.

In addition, the PDPC has introduced the Data Protection Trustmark Certification – essentially a gold star system to reward organizations with strong data protection practices, providing a competitive edge for companies (particularly helpful for vendor pitches, adding an important string to an organization's bow).

In the area of enforcement, the Active Enforcement Framework has been introduced to "motivate" organizations to develop and implement accountable practices. Under the framework, upon discovering that a data breach has occurred, an organization can now approach the PDPC with an undertaking, avoiding the threat of protracted investigations hanging over their head. The undertaking will be accepted by the PDPC provided that the organization's breach management plan is implemented and it achieves a similar or better outcome than an investigation.

Providing a second new option, organizations now also have the ability to request for an expedited breach decision from the PDPC (provided that the organization swiftly admits to the breach). Again, this avoids the unpleasantness of a protracted investigation and enables an organization to put clear-cut breaches behind them. With the matter concluded, an organization can adopt a consistent message to employees and customers without worrying that any statements made could prejudice an ongoing investigation.

Finally, in addition to the *Guide to Accountability*, the PDPC has introduced a variety of tools to help organizations both protect, and make the best use of, their data. These include the *PDPA Assessment Tool for Organizations*, the *Guide to Data Protection Impact Assessments*, and the *Guide to Managing Data Breaches*, along with a number of open source RegTech tools to help map and keep track of how personal data is being managed within an organization. As of 15 July 2019 the overarching *PDPA Advisory Guidelines* have also been helpfully updated. The PDPC has certainly been busy.

Beyond the red dot

Now more than ever, data is a global issue. It makes sense, then, that Singapore look beyond its own borders to facilitate, rather than hinder, cross-border data flows.

Singapore will shortly be a full participant in the APEC Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems, which comprise a set of APEC-approved requirements to demonstrate compliance and accountability. Organizations certified under the CBPR and/or PRP Systems will help establish a trusted network of accountable organizations in APEC economies, enabling the cross-border flow of data more seamlessly.

Contacts

Stephanie Keen
Office Managing Partner, Singapore
T +65 6302 2553
stephanie.keen@hoganlovells.com

Matthew Bousfield
Counsel, Singapore
T +65 6302 2565
matthew.bousfield@hoganlovells.com

www.hoganlovells.com