

## Media Release

FOR IMMEDIATE RELEASE

### **PERSONAL DATA PROTECTION COMMISSION INTRODUCES THREE INITIATIVES TO STRENGTHEN ACCOUNTABILITY AMONG ORGANISATIONS AND ENCOURAGE DATA INNOVATION**

*Launch of data portability and data innovation provisions public consultation, new Active Enforcement Guide and updated Guide to Managing Data Breaches 2.0*

**SINGAPORE – 22 May 2019:** The trusted use of data is the foundation of a strong Digital Economy, especially given the increased volume of personal data generated through customer activities and used to enhance products and services. While a nimble and forward-looking regulatory approach to data protection will provide an environment to build trust and facilitate innovation, organisations must shift from compliance to accountability in the management of personal data. This includes taking responsibility for how organisations use data collected from individuals, and proactively putting in place measures to safeguard such data.

The Personal Data Protection Commission (PDPC) today introduced three new initiatives to facilitate the movement and use of data to support innovation, and to strengthen accountability among organisations:

- 1) A public consultation to seek views on proposed data portability and data innovation provisions, as part of the review of the Personal Data Protection Act 2012 (PDPA);
- 2) A new Guide on Active Enforcement as part of its drive for organisations to shift from compliance to accountability; and
- 3) An updated Guide to Managing Data Breaches 2.0, to help organisations manage and respond to data breaches more effectively.

These were announced by Deputy Commissioner of PDPC, Mr Yeong Zee Kin at the “Know Ahead to Stay Ahead - Leadership’s Engagement in Data Protection” session. The event, co-organised by the PDPC and Singapore Business Federation, and supported by the Law Society of Singapore, is part of Singapore’s week-long Privacy Awareness Week, a global initiative by the Asia Pacific Privacy Authorities.

Mr Yeong said, “Data is a key enabler of digital transformation, but a balance must be achieved between data protection and business innovation. We are taking firm steps to position Singapore as a trusted data hub in the global Digital Economy by seeking feedback on the proposed data portability and innovation provisions, as well as test-bedding data breach notification measures. The PDPC also recognises the importance of being responsive and agile in enforcing data protection in an environment of fast-evolving data use, coupled with sweeping technological advances. Hence, the PDPC has converted its knowledge and experience in investigations to practical enforcement approaches in a Guide to Active Enforcement which businesses can refer to, and also updated the Guide to Managing Data Breaches.”

### **Data Portability and Data Innovation Provisions Public Consultation**

Firstly, the PDPC launched its third public consultation under the ongoing review of the PDPA, to seek feedback and views on the proposed introduction of the data portability and data innovation provisions. This consultation builds on the data portability discussion paper launched in February 2019.

The proposed data portability provision will provide individuals with greater control over their personal data and enable greater access to more data by organisations to facilitate data flows and increase innovation, while the proposed data innovation provision makes it clear that organisations can use data for appropriate business purposes without individuals’ consent. Collectively, the proposals provide a balanced

regulatory approach to empower consumer choice and support innovation in a Digital Economy.

This approach is aligned with a global push towards data portability, with jurisdictions such as the European Union, Australia, India, Japan and New Zealand either having implemented or planning to implement data portability in their respective data protection regimes. Such alignment is crucial to ensuring that the PDPA keeps pace with progressive global developments and go towards strengthening international recognition of Singapore's data protection regime.

The public consultation is open for six weeks starting today and will end on 3 July 2019. For more details, please refer to [Annex A](#).

### **Guide to Active Enforcement**

Secondly, the PDPC has introduced its new guide to Active Enforcement, which articulates its approach in deploying its regulatory powers to act efficiently and effectively when dealing with data breaches to safeguard the public interest.

The PDPC has introduced a new **expedited decision** process to bring investigations on clear-cut data breaches to a conclusion quickly. The process draws on data breach cases in the last four years and feedback from stakeholders. To be eligible for handling under the new expedited decision process, cases must meet certain conditions. These include:

- The nature of the data breach is similar to precedent cases with similar categories of facts; and
- Where there is an upfront admission of liability for breaching the PDPA by the organisation.

In expedited decision cases where financial penalties are involved, the organisation's admission of its role in the incident will be taken into consideration as a strong mitigating factor. Examples of cases eligible for the process include common forms of data breaches such as URL manipulation, poor password management, or printing errors resulting in incorrect recipients.

However, the PDPC is also aware that even companies that are well prepared may not eliminate all risk of data breaches. As such, organisations that can demonstrate to the PDPC that they have in place proper accountability practices, monitoring and remediation plans – such as Data Protection Trustmark-certified<sup>1</sup> organisations – can request to the PDPC for an **undertaking** option in the case of a data breach. The undertaking is a written promise by the organisation that it is ready to execute a fully developed and prepared contingency plan to resolve a data breach when it has occurred; or where the PDPC assesses that an undertaking would achieve a similar or better enforcement outcome as opposed to a full investigation.

The Active Enforcement guide also includes examples and clarifications to address common queries from companies such as policy considerations by the PDPC when deciding to initiate or discontinue an investigation, as well as financial penalty assessment factors.

## **Guide to Managing Data Breaches 2.0**

Lastly, the PDPC has also updated its existing guide to better support organisations in managing data breaches effectively. Under the Guide to Managing Data Breaches 2.0, organisations should have in place monitoring measures to provide early detection

---

<sup>1</sup> For more information and a full list of Data Protection Trustmark-certified organisations, please visit [www.imda.gov.sg/dptm](http://www.imda.gov.sg/dptm)

and warning for possible data breaches, and a data breach management plan for reporting and assessing a data breach.

The guide also sets out the steps that organisations can take in responding to a data breach, which include:

- **Containing** the breach to prevent further compromise of personal data
- **Assessing** the risks and impact of the breach
- **Reporting** the breach to the PDPC and informing affected individuals if necessary
- **Evaluating** response to the breach and reviewing actions taken to prevent further data breaches

The guide also updates recommendations in two main areas: (i) thresholds for notifying the PDPC and individuals of a data breach, and (ii) the timeliness of notification. Notification thresholds are expanded to consider large numbers to be where 500 or more individuals are affected, or where significant harm or impact to the individuals is likely to occur due to a breach. The PDPC also recommends that organisations conducting internal investigations and assessments of a potential data breach take no more than 30 days from when they are aware of a potential breach, and if data breach notification thresholds are met, to then notify the PDPC no later than 72 hours from the time they have completed their assessment<sup>2</sup>.

PDPC has updated these areas to incorporate feedback from prior consultations, and will monitor and adjust them as necessary. Organisations are urged to consider taking up this approach as this will allow them to respond to data breaches confidently and prepare for the PDPC's planned introduction of a mandatory breach notification in its upcoming Act Amendment. PDPC also welcomes feedback from organisations that

---

<sup>2</sup> Data intermediaries should report potential data breaches to their main organisation no later than 24 hours from when they first become aware of a potential data breach

have implemented these changes in order to make further improvements before breach notification becomes mandatory.

Both guides can be downloaded online at [www.pdpc.gov.sg/paw2019](http://www.pdpc.gov.sg/paw2019).

**Resources:**

**Annex A: Factsheet on PDPC's Public Consultation on the Proposed Data Portability Obligation and Data Innovation Provisions**

---

**ISSUED BY THE PERSONAL DATA PROTECTION COMMISSION**

---

**About Personal Data Protection Commission**

*The PDPC administers the Personal Data Protection Act 2012 (PDPA) in Singapore, which aims to safeguard individuals' personal data against misuse and promote proper management of personal data in organisations. The PDPA enhances Singapore's competitiveness and strengthens our position as a trusted business hub, putting Singapore on par with the growing list of countries with data protection laws. For more information, please visit [www.pdpc.gov.sg](http://www.pdpc.gov.sg).*

**About Privacy Awareness Week**

*Privacy Awareness Week (PAW) is an initiative held annually in May by the Asia Pacific Privacy Authorities to promote awareness of privacy and personal data protection issues. Each authority nominates a week for its country to raise awareness of the issue. In its fifth year, 2019's theme is "Protecting Personal Data is Everyone's Responsibility", and Singapore will be focusing on breach management, enforcement, and raising awareness that both organisations and individuals have a role to play in protecting personal data as companies move from compliance to accountability. Singapore's chosen week is between 18 to 25 May. Check out PDPC's PAW webpage on [www.pdpc.gov.sg/paw2019](http://www.pdpc.gov.sg/paw2019) for more information.*

**For media clarifications, please contact:**

Eugene NEUBRONNER (Mr)  
Manager, Communications and Marketing,  
Personal Data Protection Commission  
c/o Infocomm Media Development Authority  
DID: (65) 6211 1182  
Email: [Eugene\\_NEUBRONNER@imda.gov.sg](mailto:Eugene_NEUBRONNER@imda.gov.sg)

LIOW Ruo Yu (Ms)  
Assistant Manager, Communications and Marketing,  
Personal Data Protection Commission  
c/o Infocomm Media Development Authority  
DID: (65) 6751 2828  
Email: [LIOW\\_Ruo\\_Yu@imda.gov.sg](mailto:LIOW_Ruo_Yu@imda.gov.sg)



CHUA Hian Hou (Mr)  
Deputy Director, Communications and Marketing,  
Personal Data Protection Commission  
c/o Infocomm Media Development Authority  
DID: (65) 6202 4956  
Email: [CHUA\\_Hian\\_Hou@imda.gov.sg](mailto:CHUA_Hian_Hou@imda.gov.sg)