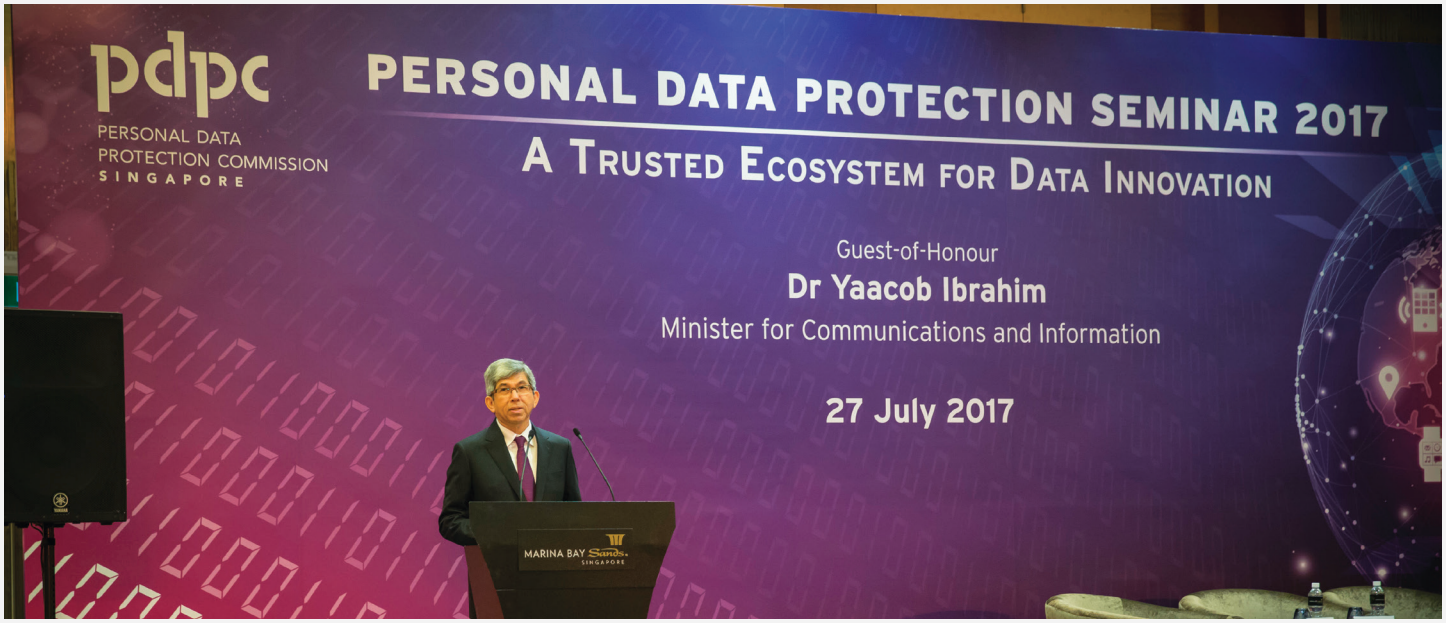

Caption: Guest-of-Honour Dr Yaacob Ibrahim delivering the Opening Remarks at the PDP Seminar 2017.

A Trusted Ecosystem for Data Innovation

Launch of the first of a series of public consultations on proposed amendments to the Personal Data Protection Act (PDPA), plans to introduce a Data Protection (DP) Trustmark certification scheme, application to participate in the APEC Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems — these were some of the key announcements made by the Minister for Communications and Information, Dr Yaacob Ibrahim, at the 5th Personal Data Protection (PDP) Seminar that was held at Sands Expo and Convention Centre, Marina Bay Sands, on 27 July 2017.

Robust and Progressive Data Protection to Support Innovation

The advancement of technologies had given rise to the ability to collect, analyse and share large amounts of data for economic and societal benefits. Data innovation and building digital capabilities had been identified as the linchpin of Singapore's strategy for growing the digital economy and becoming a smart nation. To truly realise the potential of data however, a trusted data ecosystem where organisation could thrive and individuals felt assured that organisations are collecting, using and protecting their data responsibly is crucial.

To ensure that Singapore's regulatory environment kept pace with evolving technology, yet at the same time continued to safeguard individual's personal data, the Personal Data Protection Commission (PDPC) had started to explore future-ready enhancements to the PDPA to allow for a more progressive approach to collecting, using and disclosing personal data, while also providing for greater transparency when data breaches occur. The first tranche of proposed amendments to the PDPA, which would permit organisations to collect, use or disclose personal data without consent if the situation is impractical, non-desirable or inappropriate, as well as the introduction of a mandatory data breach notification framework, had been put up for public consultation. "Notification will enable affected individuals to better protect themselves by taking some action, and allow affected organisations to receive guidance from the PDPC on how to manage the breach," said Dr Yaacob. He assured that PDPC would build in thresholds so that this requirement does not become an unnecessary burden to organisations.

In addition, the PDPC had also issued a Guide to Data Sharing which provided clarity on how organisations can share personal data, recognising that there may be circumstances where obtaining consent for the sharing of data could be impractical or undesirable. The

Guide includes the introduction of a regulatory sandbox that allows organisations to apply for data sharing arrangements (DSAs) that would be exempted from one or more obligations under the PDPA, subject to certain criteria and on a case-by-case basis. The regulatory sandbox allows organisations to testbed the enhanced framework for collection, use and disclosure of personal data that are introduced in the consultation paper, for real world usage before the amendments to PDPA are effected.

These DSAs still uphold responsible data sharing. Under the DSAs, the PDPC can still establish terms and conditions, such as having the organisations conduct a data protection impact assessment to evaluate the risks and impact to individuals of the intended sharing of personal data, or allowing individuals to opt out from sharing their personal data under the DSA.

Embedding Trust in Data Innovation for a Competitive Edge

"Even as we urge businesses to be accountable for the data they collect and use, we also want to urge them to use the data meaningfully to drive growth and innovation," said Dr Yaacob. "Data, once collected, can generate value not only for the organisation collecting the data, but also for others far removed from the initial point of contact."

Dr Yaacob cited several examples of organisations that had shared data to provide better services to customers, such as the partnership between an e-commerce business and a logistics company to facilitate doorstep deliveries. "Companies that collaborate can achieve so much more for their customers," he added. He further clarified that that the PDPA does not prohibit the sharing of personal data, and that "we want to encourage the responsible sharing of personal data in order to generate value for our economy."

The interplay between data protection, data sharing and data innovation was discussed at great length during the first panel of the morning sessions. The biggest challenge for organisations in data sharing, as it was noted, is to find ways to do this while engendering trust. Moderating the first panel discussion, Professor Simon Chesterman, Dean, Faculty of Law, National University of Singapore, commented that reputations could be lost very quickly – possibly within nanoseconds in a digital economy – if organisations misuse or lose data.

Sharing Singtel's experience of how the company innovated and remained competitive through the use of customer data without losing their trust, Ms Wu Choy Peng, Group Chief Information Officer, explained that a lot of the customer data is used for operational purposes such as the planning of network deployment to improve coverage or ensuring relevant product

DPO Connect August 2017
PDPC PERSONAL DATA PROTECTION COMMISSION SINGAPORE

and promotion offerings to suitable customers. However, the telecommunications company drew the line at selling customer data. "Very early on, Singtel and our subsidiary Optus discussed that our primary objective is not to make money by selling customer data. By doing that, it erodes the trust of customers, and losing our core subscriber base will cost us far more than whatever little money we can make from commercialising our customer data."

For Facebook, a key factor in the growth of its data-driven services had been its ability to build "trust", said Mr Stephen Deadman, Global Deputy Chief Privacy Officer. And the crux of this matter with trust, was data. "It is about how you, as a citizen or consumer interface with the organisation, and understand how your data is being used, and the degree of control or consent that you have."

"The crux of the trust question is data. It is about how you as a citizen or consumer interface with the organisation and understand how your data is being used, and the degree of control or consent that you have."

- Mr Stephen Deadman,
Global Deputy Chief Privacy Officer, Facebook

While personal data protection was something that Facebook had invested in from the early days, it still constantly tries to understand how people engaged its systems to help them better protect their personal data. For example, the company had applied design thinking to the way users refer to the terms and conditions regarding the collection, use and disclosure of their data. Here, the challenge was to develop user interfaces and processes that help users understand how their data is being used and the degree of user control or consent that is involved, given the short span of attention that these users are likely to devote to digesting those terms and conditions.

Providing another perspective on the challenges involved, Dr Du Yuejin, Chief Security Expert and Vice President of Security, Alibaba Group, said a lot needs to be done to enhance the capabilities of organisations, especially small and medium enterprises, in the area of data protection. "Data is flowing in a very complicated supply chain, and we need to protect the data in that chain." To address this, Alibaba Group had introduced its Data Security Maturity Model[i] to the industry, to help partners and key players of the ecosystem address personal data protection and other data security issues.

Pivoting from Compliance to Accountability

In his speech, Dr Yaacob also urged organisations to view data protection as a responsibility to be fully integrated into the organisational culture of stewardship and accountability, and not merely as a compliance exercise. "This mindset shift is essential to build trust with their customers," he said.

Elaborating on the resources that PDPC would be rolling out to help organisations make the transition, PDPC Commissioner, Mr Tan Kiat How, announced that a Guide to Developing a Data Protection Management Programme (DPMP) and a Guide to Data Protection Impact Assessments (DPIAs) would be published later in the year. Additionally, PDPC would be introducing an interactive online tool that organisations may use to identify gaps in their data protection policies and practices, accompanied by actionable suggestions and recommended resources that organisations can turn to, to address the shortcomings. "These are accountability and data protection design tools which adopt sensible, risk-based approaches towards data protection", he pointed out.

The Data Protection (DP) Trustmark certification scheme, which could function as an indicator of a business' sound data protection practices and processes, was another such mechanism, said Dr Yaacob. Aimed at encouraging organisations to be transparent and accountable in their data protection measures, the scheme was expected to be launched by the end of 2018.

[i] The Data Security Maturity Model (DSMM) is a multi-level maturity model for organisations to measure their data security capability maturity level, identify issues related to data security capability, and improve their data security capability.

"Data is flowing in a very complicated supply chain, and we need to protect the data in that chain."

- Dr Du Yuejin,
Chief Security Expert and Vice President of Security, Alibaba Group

Facilitating International Data Flows

Cross-border data flows had been showing an uphill trend in the digital economy. In Singapore, the direct value added to the country's gross domestic product (GDP) of data connectivity in trade was estimated to be around 40 per cent, with the numbers expecting to rise further. "As they do, the international community will demand higher cross-border data protection standards so that customers and businesses overseas can exchange data with Singapore with the assurance that we will use the data responsibly," said Dr Yaacob.

To facilitate responsible and more seamless sharing of data across borders, Singapore had just submitted its Notice of Intent to participate in the APEC CBPR and PRP systems. Through harmonised standards across participating economies, businesses could "enjoy more clarity, save on the costs of ensuring compliance with multiple standards across different economies, and retain consumer confidence in the responsible handling of their data". Dr Yaacob added that PDPC would align its DP Trustmark standards with that of APEC CBPR and APEC PRP so that organisations that obtain one will concurrently be certified under the other.

The need for enabling data transfers and the economic benefits of APEC CBPR were discussed in greater depth at the second panel discussion of the PDP Seminar that was moderated by Mr Derek Ho, Vice-President of AsiaDPO.

Imparting his views on why countries should get on board the APEC CBPR, Mr Ben Gerber, Chief Information Security Officer and Chief Privacy Officer of South Korean e-commerce platform Coupang described that as "the most practical way to facilitate cross border data flow". He explained that the framework allows organisations to provide assurance and confidence to the public and the regulator "where the rubber hits the road". It also provided an opportunity for economies that are tied to a "prescriptive checkbox compliance approach" to data protection, to look at the risk-based approach that APEC CBPR offers.

Caption: PDPC Commissioner Tan Kiat How speaks on accountability and data protection design tools in adopting a risk-based approach towards data protection.

DPO Connect August 2017

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

"The (APEC CBPR) framework allows organisations to be held accountable to the public and the regulator where the rubber hits the road."

- Mr Ben Gerber,
Chief Information Security Officer and Chief Privacy Officer, Coupang

Sharing Japan's experience in facilitating international data flows, Dr Kaori Ishii, Associate Professor, Graduate School of Library, Information and Media Studies, University of Tsukuba, spoke about the evolution of the Japanese Personal Information Protection Act, which was introduced in 2003 and amended in 2015 to include a provision for international data transfer. Other initiatives undertaken by Japan were its participation in APEC CBPR and its cooperation with the European Union to boost secure data transfers.

Growing Year on Year

This year's PDP Seminar, which attracted close to 800 participants, was the first to feature a full-day format with panel discussions taking place in the morning, followed by afternoon workshops that provided practical guidance on what organisations can do in the event of a data breach, as well as the good practices they can develop as part of their accountability approach, such as data protection management programme and soft skills and mediation.

Following the adoption of the ASEAN Framework on Personal Data Protection in November 2016 at the 16th ASEAN Telecommunications and IT Ministers meeting (TELMIN), PDPC and Japan's Ministry of Internal Affairs and Communications (MIC) jointly organised an ASEAN-Japan workshop in the afternoon of 27 July 2017 to discuss the importance of Personally Identifiable Information (PII) protection in ASEAN and the way forward. Co-chaired by PDPC's Executive Chairman (DPAC) Mr. Leong Keng Thai and MIC's Director General Mr. Seiji Takagi, the workshop was attended by more than 30 delegates from 9 ASEAN Member States and Japan.

New Resources for Organisations

- **Guide to Developing a Data Protection Management Programme (DPMP)**
- **PDPA Assessment Tool for Organisations (PATO)**
- **DP Advisor**
- **Guide to Data Protection Impact Assessments (DPIAs)**
- **DP Starter Kit**
- **PDP Digest**