

**KEYNOTE ADDRESS BY MINISTER JOSEPHINE TEO AT PERSONAL DATA
PROTECTION SEMINAR 2022
ON 20 JUL 2022**

1. Good morning and thank you for inviting me.

In the past decades, we have set up a progressive data protection regime that supports growth

2. If there is anything common between oil, utilities, and nuclear waste, the answer will not be immediately obvious. In fact, they have *all* been used to describe data, the subject of our seminar today.
3. There may never be a perfect analogy for data. But like oil, data need to be processed before they become useful. Unlike oil however, data does not deplete. Like utilities, there must be infrastructure to enable reliable access. But unlike utilities, data invoke a much stronger sense of ownership. You and I will not want to share data the way we might with water or electricity, even for a price. When data is mishandled, the damage can be irreparable, not unlike nuclear waste. There are other analogies for data. But the above illustrate the importance of data in the digital era. They also remind us that data as a valuable resource needs good governance.
4. In this regard, Singapore's journey began some two decades ago, back in 2002. Back then, households were just transiting from dial-up Internet connection to broadband. E-commerce markets were in its infancy but already attracting consumers. Businesses participating in international trade already needed to transmit data efficiently across borders. New concerns and questions emerged. How can individuals be protected over the internet? How can businesses transmit data across borders securely? That year, the National Internet Advisory Committee issued the voluntary Model Data Protection Code for the Private Sector based on internationally recognised principles. It was Singapore's first step in setting out the key principles for our data governance regime. Even then, we recognised the importance of supporting the data needs of businesses, whilst ensuring that consumers' personal data were protected.

5. In the decade that followed, the number of internet users globally more than doubled. Consumers swapped their mobile phones for smartphones. In the 2010s, the soaring popularity of apps like Facebook, YouTube and WhatsApp brought about new concerns.
6. The voluntary Code was no longer sufficient. Singapore needed a comprehensive data protection law. In 2012, the Personal Data Protection Act, or the PDPA, was passed in Parliament, setting a baseline standard for data protection across the economy.

We are strengthening accountability, supporting access and building partnerships

7. Over the years, Singapore has been consistent in our pursuit of our twin objectives for data protection: one, to ensure adequate safeguards for consumers' personal data; two, to strengthen Singapore's economic competitiveness and status as a trusted data hub.
8. With increased digitalisation across all aspects of our daily lives, we do not assume that both objectives will continue to be met. Let me now share the three *principles* that will continue to guide us.
9. **The first principle is accountability.** Organisations need to take responsibility for the personal data they collect and manage. There is now a growing awareness among businesses that good data protection makes good business sense. Consumers cannot be expected to trust their personal data to businesses that do not take their responsibility seriously. In 2019, we introduced the Data Protection Trustmark to certify businesses that meet the highest data protection standards. The Trustmark certification also makes the organisation's commitment visible to consumers. One familiar name among those already certified is Grab, the first superapp¹ company in Singapore to have done so. It has joined the ranks of businesses like DBS, M1 and Great Eastern Life, which have all invested in data protection to build consumer trust. To date, more than 100 businesses across diverse sectors have been certified, covering over 38,000 employees and 70 million personal data records of their stakeholders. We look forward to more businesses being certified.

¹ A superapp is a mobile or web application that can provide multiple services like payment and financial transaction processing. It can become a self-contained commerce and communication platform that embraces many aspects of personal data commercial life.

10. Beyond certification, regulations also have to keep up. In 2020, the Government amended the PDPA to provide greater clarity and support for organisations seeking to use personal data for business improvement or innovation. With adequate safeguards, they can use personal data without having to seek additional consent. This has helped businesses to use data to better understand their customers, improve their goods and services, and enhance operational efficiencies.
11. **The second principle is accessibility.** Businesses may not have a legal expert or a sizeable budget to comply with the PDPA. Over the years, we have made more tools and guidance accessible, so that businesses can comply with greater ease. Last year, I launched the Better Data Driven Business programme. It offers a free business intelligence tool that can be used to meet objectives like promoting sales growth. At the same time, data protection measures are built into the tool, so businesses can use data confidently. This year, businesses can enjoy an expanded range of easy-to-use tools: SMEs can sign up for the Data Protection Essentials programme², which provides security solutions and one-stop professional services. Georges Group, an F&B company, is one of the first to try. It found the onboarding process smooth. With the right systems and processes in place, it is now more confident in collecting personal data. You may also be familiar with the Do Not Call Registry Application Programming Interface, or API, which allows businesses to integrate “Do Not Call” checks into their calling systems. The API has made it easier for companies like Amicus and SpiderGate which provide direct marketing systems to assure their clients that consumers on the Do Not Call Registry will not be called by accident.
12. **The third principle is partnerships.** The number of countries that have data protection laws have grown from a handful at the turn of the 21st century, to over 70% of countries today. This may sound like a plus for consumers but for businesses, it can be a nightmare trying to comply with many different legal requirements when moving data across borders. A progressive, internationally recognised data protection standard is likely to top your wish list. This is why we are working with regional partners to build convergence on norms that support data flows. For example, since 2021, businesses across ASEAN countries have had access to the ASEAN Model Contractual Clauses. These are contractual terms recognised by all ASEAN Member States which businesses can use for inter-company transfers of personal data across

² This was announced in Minister’s COS speech this year.

borders. For businesses which need inter- and intra- company transfers across a wider region, we have the APEC Cross Border Privacy Rules system, or CBPR. This certification bridges differing privacy laws in APEC, reducing barriers to data flows. We are also working with partners to take the CBPR system global. This means possibly, one common certification for data transfers across many economies in and beyond APEC, making seamless global data flows a real possibility. Singapore is one of the founding economies of the Global CBPR Forum. In addition, we are working with the UK on a mutual agreement to enable even more seamless data transfers at the country-to-country level.

In the next decade, we will continue working closely with industry to unlock the potential of data and ride the wave of innovation

13. We have made encouraging progress in the two decades of Singapore's data governance journey. I am heartened to note that today, close to 90% of businesses agree that the PDPA helps them prepare for the Digital Economy. More than 80% of consumers say that it gives them confidence that their personal data is protected from misuse by organisations.
14. What will the next decade hold? How can we address emerging challenges and risks that arise with new technologies?
15. We foresee the Government, industry and the people sectors working even more closely in two priority areas:
 - a. **Building common data infrastructure**; and
 - b. **Developing Privacy Enhancing Technologies**, or PETs.
16. One example of common data infrastructure is SGTraDex, which allows stakeholders in the supply chain ecosystem to exchange data easily in a secure environment. SGTraDex is borne out of a partnership between the key players in the public and private sectors that see the need for such a secure data highway.
17. As for PETs, this is borne out of the need to harness technology itself to strengthen data protection. This includes investing in tools and processes that enable businesses to extract value from data without exposing the data itself. PETs provide businesses the opportunities to develop useful AI systems. For instance, banks can pool data and

build AI models for better fraud detection, while protecting their customers' identity, as well as financial information.

18. Today, I am pleased to announce the launch of the PET Sandbox. This is another step forward to help businesses to pilot PETs when they use data on their own or in partnerships with other entities. We will start with a focus on three common business challenges where there are privacy concerns: How to identify common customers across business units? If you have different business units and they all know something about a customer, how do you enable the pooling of such data so that you can develop a more holistic picture of the customers. How to establish a more holistic picture of the customer preferences? How to make the data accessible for AI development?
19. Businesses participating in the PET sandbox will have access to a panel of PET solution providers and enjoy a comprehensive suite of support. This includes grants to develop the solution and regulatory guidance. One of our PET solution providers is known as BetterData.ai, it converts real data into realistic synthetic data that retains the insights of the original data. This can be game-changing for businesses as we can all imagine. Data can be used safely to generate insights and develop AI models as the data does not relate to any individual.
20. Our learnings from the sandbox will in turn inform our policies and help set standards and best practices. This will also promote the development of a safer and more innovative data ecosystem for all.

Conclusion

21. To conclude, data when used well can unlock many possibilities. Let us continue to be guided by the principles of strengthening accountability, supporting accessibility, and partnering like-minded stakeholders in our use of data.
22. I wish you all an insightful and fruitful discussions ahead. Thank you.

+++