

**Privacy Commissioner's Speech at**  
**Philippines' National Privacy Commission's**  
**6<sup>th</sup> National Data Privacy Awareness Week Conference**

*25 May 2023*

**Greetings**

1. Good afternoon, Commissioner Naga, colleagues of the National Privacy Commission (NPC), ladies and gentlemen. Thank you for inviting me to speak at this conference. I am very honored, and excited, to join you at today's conference as this is the first event organised by the NPC in which we participated since the execution of the MoU between the NPC and the Hong Kong PCPD on Monday, three days ago. So, Commissioner Naga, we are losing no time in implementing the MoU to share and learn from each other's experience!

**The value of data privacy in the digital age**

2. As you are aware, the values of data and data privacy have been increasingly important in recent years. While we are

enjoying the fruits brought by emerging technologies, such as generative AI systems and powerful chatbots like ChatGPT, these technologies also bring with them inherent privacy and ethical risks. These potential risks call for clear data privacy safeguards, and the secure, responsible and ethical use of data, in particular, personal data, must be a priority for all organisations.

### **Importance for organisations to develop and implement a privacy management program (PMP)**

3. One way to achieve this is through the development of a privacy management program, also known as the PMP, which my office, the PCPD, has been advocating all along.
  
4. A PMP is about making a conscious business decision and change for the company's customers starting from the board room. A PMP, if designed and implemented properly, can help companies garner trust from their customers and other stakeholders. This would in turn bring long-term benefits to the company's overall competitiveness, reputation and goodwill. In other words, a holistic PMP strategy can lay the

bedrock for good data governance, business sustainability and growth.

### **The 3 core elements of PMP that the PCPD has advocated**

5. An effective PMP is about implementing an accountability framework that entails the responsible collection, holding, processing and use of personal data. My office has been advocating 3 core components.
6. Firstly, there should be organisational commitment with an internal governance structure in place that fosters a culture respectful of personal data privacy. This would often require the organisation to adopt a top-down approach, with a specific reporting mechanism set up with respect to the handling of data breach incidents and with a dedicated data protection officer appointed to report on data issues to the top management.
7. Secondly, there should be appropriate programme controls in place. The controls that we recommend range from establishing a personal data inventory and internal policies

on personal data management and the handling of data breach incidents, to adopting risk assessment tools, and having effective training and communication channels in place.

8. Finally, there should be ongoing assessment and revision of the PMP to keep it in pace with the changes both within and outside the organisation. This is particularly important given the ever-rising expectation of customers nowadays and the fast-changing digital innovations which we are experiencing every day.

### **PCPD's work on PMP since 2014**

9. Since 2014, my office has been encouraging organisations to develop their own PMPs so that they can embrace personal data protection as part of their data governance responsibilities and apply it as a business imperative throughout the organisation.

10. To this end, my office has published a “Best Practice Guide” in August 2018 to assist organisations in developing

a practical and comprehensive PMP framework. Apart from organising regular professional workshops for businesses and industry stakeholders to learn more about the benefits of implementing a PMP, my office has also formed a Data Protection Officers' Club <sup>1</sup> to provide practising data protection officers with a platform to enhance their knowledge and build up their expertise of data privacy compliance through experience sharing and training.

11. The launch of the Privacy-Friendly Awards by my office in 2021 has further demonstrated the PCPD's efforts in encouraging organisations to embrace the protection of personal data privacy as part of their organisation policy and culture. The Awards aim to recognise the commitment and efforts of enterprises, public and private organisations as well as government departments in protecting personal data privacy. I am glad to share with you that the 2021 Awards received an overwhelming response with 100 organisations being awarded. With the launch of the 2<sup>nd</sup> Privacy-Friendly Awards this year under the theme of "Embrace Privacy Management Programme to Gain Trust and Benefits", we

---

<sup>1</sup> DPOC was established in 2000: <https://www.pcpd.org.hk/misc/dpoc/about.html>

envisage that more organisations in this round, namely, over 100 companies or organisations, would be recognised for their work in protecting data privacy and in incorporating a PMP in their respective organisations.

### **Significance of having PMP for organisations**

12. Looking forward, I strongly believe that the protection of personal data privacy should not be seen and dealt with as a mere compliance issue. It is not only about “taking a box” off the compliance checklist. Rather, it is about adopting a proactive approach in bringing a data-privacy friendly culture into the business equation, in order to garner the necessary trust from customers for the benefit of the organisation.

### **Concluding Remarks**

13. The theme for this year's conference is “Empowering DPOs and Protecting Personal Data Privacy Rights of Filipinos”. As Commissioner Naga pointed out at the signing of the MoU between the NPC and the PDPC, the

signing of the MoU reaffirms both authorities' firm belief that robust data governance is essential to protecting data subjects' privacy rights, ensuring trust in digital services and harnessing the transformative potential of data for social and economic progress.

14. Indeed, the signing of the MoU shows our joint commitment and dedication in safeguarding personal data privacy of citizens in our respective jurisdictions. I believe that the enhanced collaborative efforts of both authorities would facilitate the growth and development of digital economies in both jurisdictions while safeguarding personal data privacy. Going forward, I am confident that the two authorities can share our expertise and experience in areas of mutual interests amidst rapid technological developments in both jurisdictions.

15. With that, I wish you all an insightful and fruitful conference. Thank you.