Hong Kong China Network Security Association
Symposium: The 2026 Annual Cybersecurity Forum
"Compliance vs. Achieving Business Objectives:
From Data Privacy to AI Governance"
25 June 2026

Opening Address by Ms Ada Chung Lai-ling,

the Privacy Commissioner for Personal Data

Chairman David (Founding Chairman of the Hong Kong China Network Security Association, Mr David Ip); Commissioner Francis (Commissioner of Critical Infrastructure (Computer-system Security), Mr Francis Chan); Cari (Acting Deputy Commissioner (Digital Infrastructure) of the Digital Policy Office, Ms Cari Wu); Sidney (Assistant Director (Regulatory) of the Office of the Communications Authority, Mr Sidney Tsan); Raymond (Chief Superintendent of the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force, Mr Raymond Lam), ladies and gentlemen,

1. Good morning. It is a great pleasure for me to join you today at the 2026 Cybersecurity Forum organised by the Hong Kong China Network Security Association. I am delighted to open this event as we chart a course for sustainable innovation rooted in trust.

2. We are meeting at a pivotal moment in the digital age, where data, including personal data, have become the currency of modern economies and the lifeblood of artificial intelligence (AI). Evolving at an unprecedented pace, AI is rapidly shaping how we innovate, compete, and grow. In just a few years, AI has evolved from a tool to assist human decision-making to increasingly autonomous systems capable of performing tasks independently.

3. Globally, AI has been the focus of attention in virtually every conference and discussion. I think that at this stage, the global community has reached a consensus regarding AI: namely that the development of AI is irreversible and that its development or use carries inherent risks, particularly in terms of privacy protection. Indeed, our Country's 15th Five-Year Plan gives equal

importance to development and security, and Hong Kong is actively promoting the "AI plus" initiative, which envisions a broad and deep integration of AI across all sectors, in line with national policy.

4. For Hong Kong, the question is therefore not "whether" we should develop or use AI, but "how" we should do so, and more specifically how to "foster a beneficial, safe and fair digital and intelligent development environment".

5. In this context, a familiar question keeps coming up: Can businesses pursue innovation and growth, while meeting the requirements of data protection and responsible AI governance?

6. For some, compliance is perceived as a hindrance to innovation. But we must move beyond this outdated dichotomy and rethink the true meaning of compliance. Today, I invite you to consider another perspective: rigorous data protection and strong AI governance are not incompatible with business success; they are the very foundation of sustainable growth.

7. Today, compliance is no longer a reactive approach, a checklist to be completed after innovation has taken place. In a data-driven economy, trust is not incidental; it is fundamental. Customers are more demanding. Partners are more cautious. Global data flows are increasingly dependent on adequate safeguards. In this environment, organisations that consider privacy and governance as peripheral will struggle to remain competitive. Conversely, those that integrate the principles of privacy and governance, as well as accountability, transparency, and responsibility, into their core strategy send a strong signal: they are the trustworthy custodians of personal data, their systems are safe, and their innovations are reliable. The trust they inspire ultimately translates into competitive advantages.

8. This brings us to the central proposition of today's theme: the dual mission of development and security, which, as I have said, is also advocated by the 15th Five-Year Plan. In Hong Kong, the Honourable Chief Executive rightly emphasized in his Policy Address that the development of AI must be steered by safety and driven by application.

9. In this regard, we have already seen the risks: excessive collection and misuse of personal data, data leakage, opaque decision-making, bias in algorithms and inaccurate results. A recent data breach involving an online learning management platform, which was reportedly hacked, has caused significant disruption for 9,000 universities and institutions worldwide, including those in Hong Kong. It is not difficult to imagine the considerable repercussions of this incident for the operator, in terms of operational continuity, reputational damage, and costs. If left unmanaged, these risks will undermine customer trust and the success and sustainability of the organisation.

10. Regarding costs, some organisations may feel that due to a lack of resources, further investment in data security is not justified. However, it should be noted that a data breach incident can completely wipe out an organisation's market capitalisation. You may recall that as a result of a hacking attack to the Australian Medibank's information system in 2022, Medibank's market capitalisation plunged by 1.8 billion Australian dollars, or 9 billion Hong Kong dollars, in just one day. I would say losses of this nature fully demonstrate the necessity and the cost effectiveness of allocating resources to protecting your customers' data, particularly in the age of AI.

11. As the Privacy Commissioner for Personal Data, I believe that the mission of my Office is to fully uphold our commitment to privacy protection, by acting as a vigilant "guardian" while proactively embracing innovation as a forward-looking "reformer" in a world shaped by AI. As you may know, since 2021, my Office has published various AI guidelines and related publications to help organisations implement good AI governance and innovate responsibly and safely, while complying with the requirements of privacy legislation.

12. In this context, AI governance generally means having the necessary policies, regulations, and ethical guidelines to ensure that AI systems are developed and used safely and responsibly. For example, the "*Artificial Intelligence: Model Personal Data Protection Framework*" and the "*Checklist on Guidelines for the Use of Generative AI by Employees*", published by my Office, are practical references for good AI governance; they help

organisations develop or strengthen their internal policies and practices regarding the development or use of AI.

13. In the era of AI, organisations must develop AI governance strategies and integrate this governance into the entire lifecycle of AI systems, from design and development to deployment and use. This includes ensuring that training data are obtained legally, that risks are identified and assessed quickly, that human oversight is maintained, and that systems remain explainable and accountable.

14. To better understand current AI practices in Hong Kong and their impact on personal data privacy, my Office has already carried out three rounds of compliance checks since 2023, examining the use of AI by approximately 150 organisations. I am pleased to note that all the organisations reviewed have developed Personal Information Collection Statements and implemented appropriate security measures for the collection or use of personal data through AI systems. Most of these organisations have adopted the "human-in-the-loop" approach to monitoring AI systems, have put in place AI governance structures, and are gradually developing internal policies or guidelines regarding the use of generative AI by employees.

15. In addition to strengthening compliance efforts and publishing guidance materials, my Office has launched a series of promotional and educational activities aimed at promoting privacy protection in the development and use of AI. We established the HK International Data Privacy Academy just a week ago, with a view to building Hong Kong into an international hub for high-calibre privacy professionals. We are confident that the Academy will help foster a beneficial, safe, and fair environment for the continued development of AI in Hong Kong, and we look forward to collaborating with all of you to accomplish this mission.

16. Ladies and gentlemen, allow me to conclude by quoting Professor Fei-Fei Li, known as the "Godmother of AI". Professor Li stated, "In the AI age, trust cannot be outsourced to machines. Trust is fundamentally human". I would say that technology can help us innovate and improve our lives, but trust in technology must be built by humans, through responsible decisions, appropriate safeguards, and above all, respect for privacy.

17. Lastly, I would like to reiterate my thanks to the Hong Kong CNSA for this invitation and for its commitment to advancing cybersecurity industry standards in Hong Kong. I wish you a fruitful and inspiring Forum. Thank you!