IAPP HK's KnowledgeNet Sharing Session

31 March 2022 (Thursday)

Opening Address by Ms Ada CHUNG Lai-ling

Privacy Commissioner for Personal Data

---

1. Good evening, Jason (Chair of IAPP Hong Kong KnowledgeNet Chapter), ladies and gentlemen. It is my great pleasure to attend the first IAPP Hong Kong event of this year. I must say the IAPP and its chapters around the world, including the Hong Kong chapter chaired by Jason, have provided a wealth of valuable resources and insights on various privacy issues both for its members and regulators.

2. As I am aware, the theme for this evening is privacy challenges for businesses when implementing technology and process to handle COVID-related data. Indeed, for the past two years, and especially since the onset of the fifth wave in Hong Kong, organisations have had to implement work-from-home arrangements from time to time, and they are required to handle COVID-related data, mostly that of their employees.

Collection of health data from employees

3. During the pandemic, it has become more and more common for employers to collect health data from employees in order to reduce the risk of transmission of the coronavirus variants in the workplace. While employers and employees have started to take this practice for granted, our statistics suggest that such collection warrants our attention:

- In 2021, my Office received over 850 enquiries in relation to the collection of personal data from employees, among which over 330 were about the collection of employees' health data; and
- Out of 140 data breach notifications we received from organisations last year, 15% involved the leakage of employees' data.

4. For the past three months alone, my Office has received 157 enquiries relating to the collection of health data from employees. Against this background, we published a guidance note last Friday to help employers and employees in Hong Kong to understand the employers' obligations under the local privacy law, the Personal Data (Privacy) Ordinance ("the Ordinance"), when it comes to the collection and use of employees' health data during the pandemic.

5. It is generally justifiable and reasonable for employers to collect certain kinds of COVID-related health data from employees to assess the risk of coronavirus transmission in the workplace and safeguard the health of employees and visitors on their premises during the pandemic. That being said, it is also important for businesses, or employers, to note the privacy risks involved and the need to comply with the requirements of the privacy law.

6. From the enquiries made with us, for example, we note that there are instances where businesses ask for the health data, or vaccination records, of the employees' family members. In other cases, WhatsApp groups were created for all employees to submit their health data, including vaccination records, test results or infection records, to the HR department on the same platform, with all such data being shared and accessible by all members of the same group.

7. With reference to the Data Protection Principles (DPPs), which I believe are well known to most of you, we would question if, for example, the collection of the health data of employees' family members is in contravention of the data minimisation and necessity principles. Apparently, the arbitrary disclosure of the health data of an individual employee in a WhatsApp group open to all members of the group is also in breach of the limitation of use and data security principles.

8. As COVID-related data, such as health data, is generally considered sensitive, any leakage of such data may cause significant harm, including psychological harm, to the relevant data subjects. Pursuant to Data Protection Principle 4, organisations as data users shall take all practicable steps to ensure that the personal data held by them should be protected against unauthorised or accidental access, processing, erasure, loss or use. Hence, we cannot overemphasise the importance of data security in this context, especially when modern technology is deployed to process or store the data.

Vaccine Pass

9. Speaking of data security, I would like to use the example of Hong Kong's Vaccine Pass to illustrate some of the privacy-protecting features embedded in the operation of the Vaccine Pass. As you may be aware, the use of Hong Kong's Vaccine Pass now covers various types of specified premises, such as restaurants, supermarkets and shopping malls, and operators of most venues like restaurants are required to check the vaccination records of their visitors.

10. The first privacy-protecting feature is that data minimisation techniques have been adopted in the design of the Vaccine Pass. When a visitor scans the venue's LeaveHomeSafe QR code with their LeaveHomeSafe app, no personal data will be displayed on

screen and only the QR code which represents the vaccination record or medical exemption certificate will be visible. Nor will any personal data be shown on the screen of the venue operator's mobile device when they use the official "QR Code Verification Scanner" Mobile App to verify the visitor's Vaccine Pass.

11. Further, while visit records will be created after the Vaccine Passes are verified, all such records, which originate from the visitors' vaccination records and contain personal data, will be masked and hashed, resulting in the production of unidentifiable data which is then stored in the mobile device of the venue operators. The visit records will also be encrypted, making them inaccessible to the venue operators. In essence, in my view no personal data as defined under the Ordinance is stored in the mobile device of a venue operator.

12. The development of the Vaccine Pass in Hong Kong fully illustrates the importance of conducting a Privacy Impact Assessment (PIA) and the adoption of privacy-by-default in the design and development of a new device in the collection of COVID-related data. In the case of the Vaccine Pass, in addition to seeking advice from my Office, we note that the Government has engaged an independent third party to conduct the PIA in the development of the Vaccine Pass.

Artificial Intelligence

13. Indeed, given the advancement of technology, organisations nowadays increasingly adopt artificial intelligence (AI) in their operations and in the handling of data. According to a global survey by McKinsey in 2021[1], more than 50% of the organisations interviewed adopted AI in at least one function. According to a report published by the Hong Kong Institute for Monetary and Financial Research in October 2021, 71% of firms across sectors of the financial services industry in the Asia-Pacific region have either adopted or planned to adopt AI or big data technologies in the next 12 months.[2]

14. While the use of AI presents huge opportunities and benefits, it also carries inherent risks to the protection of personal data and privacy owing to its data-intensive nature. As Bill Gates said at the 2019 Human-Centered Artificial Intelligence Symposium at Stanford University, AI is "*both promising and dangerous*". Last August, my Office published the "Guidance on Ethical Development and Use of Artificial Intelligence", with a view to helping organisations to develop and use AI in an ethical manner, and to comply with the Ordinance when they develop or use AI.

---

[1] McKinsey & Company (2021), *The state of AI in 2021:* *https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Analytics/Our%20Insights/Global%20survey%20The%20state%20of%20AI%20in%202021/Global-survey-The-state-of-AI-in-2021.pdf*

[2] Hong Kong Institute for Monetary and Financial Research (2021), *Artificial Intelligence and Big Data in the Financial Services Industry – A regional perspective and strategies for talent development* https://www.aof.org.hk/docs/default-source/hkimr/applied-research-report/aibdrep.pdf

15. Expanding from three Data Stewardship Values of being respectful, beneficial and fair to stakeholders, the Guidance promulgates seven ethical principles for AI which are in line with internationally recognised principles in the field.

Work Plan of the PCPD

16. Incidentally, I would also like to take this opportunity to share with IAPP members the work and priorities of my Office this year.

17. As you are aware, we amended the Personal Data (Privacy) Ordinance last year to criminalise doxxing acts and empower the Privacy Commissioner to carry out criminal investigations and institute prosecutions in respect of doxxing-related offences.

18. I am pleased to report that our enforcement work has been very effective so far. From the commencement of operation of the Amendment Ordinance since October last year until the end of February 2022, my Office issued more than 460 cessation notices to 12 platforms to request the removal of over 2,400 doxxing messages. We made the first arrest for a suspected contravention of the new doxxing offence in last December, and initiated criminal investigations in 43 cases. Needless to say, combating doxxing remains one of our top priorities this year.

19. Other than that, we are also working with the Government in reviewing the provisions of the Personal Data (Privacy) Ordinance, with a view to formulating further legislative amendment proposals for the consideration of our Legislative Council. The directions of review include establishing a mandatory data breach notification mechanism, instituting a requirement on specifying data retention period, regulating data processors, and empowering the Privacy Commissioner to impose administrative fines.

20. For the coming year, we will forge ahead with our work on monitoring, supervising or promoting compliance with the privacy law. Last August, we issued the Guidance on the ethical development and use of AI, and we plan to do more promotion or education work this year. While we will continue to issue advisories or guidance notes on technology or COVID-related issues, children privacy is also a priority on our agenda.

21. On the international front, my office is going to host the 57th Asia Pacific Privacy Authorities (APPA) virtual forum in July this year, as one of the signature events in celebration of the 25th anniversary of the establishment of the Special Administrative Region. For those of you who are also members of our Data Protection Officers' Club, we plan to organise a discussion session on some topical issues among different DPAs (Data Protection Authorities) for the benefit of our DPOC members.

Together, let's fight the pandemic

22. To conclude, notwithstanding that Hong Kong is now facing an unprecedented public health crisis, I believe that so long as we maintain good personal hygiene, observe social distancing measures, and, most importantly, get fully vaccinated, we will weather the storm. I believe that with the strength, resourcefulness and agility of Hong Kong people, we will be able to bounce back speedily. With that, may I wish you all a very enjoyable and insightful discussion this evening.

23. Thank you.