Minutes of the 56th Meeting
of the Personal Data (Privacy) Advisory Committee
held at 12/F, Sunlight Tower, 248 Queen’s Road East, Wan Chai, Hong Kong
at 10:00 a.m. on 2 April 2019

Present
Mr Stephen Kai-yi WONG, Privacy Commissioner (Chairman)
Mr Jimmy KWOK (Member)
Mr Stephen LOH (Member)
Mr David WAN (Member)
Ms Connie LAM (Member)
Mr Addy WONG (Member)
Ms Rosanna LAW, Deputy Secretary for Constitutional and Mainland Affairs (Member)

In attendance
Mr Jacky LUM, Principal Assistant Secretary for Constitutional and Mainland Affairs
Ms Karen YIP, Assistant Secretary for Constitutional and Mainland Affairs
Mr Tony LAM, Deputy Privacy Commissioner
Ms Raina YEUNG, Assistant Privacy Commissioner (Legal, Policy and Research)
Mr Daniel LEUNG, Chief Personal Data Officer (Corporate Support)
Mr Dennis NG, Legal Counsel – for item 3 below only
Mr Alex LAI, Legal Counsel – for item 4 below only
Mr Anthony CHAN, Senior Personal Data Officer (Corporate Support) (Secretary)

Absent with apologies
Ms Winnie YEUNG (Member)
Ms Cordelia CHUNG (Member)
1 Minutes of the last (55th) meeting held on 5 December 2018 (Paper No. 01/19)

1.1 The Committee confirmed the minutes of the last meeting held on 5 December 2018, which had incorporated all the amendments made by Members.

2 Matters arising from the minutes of the last (55th) meeting

Update on the European Union General Data Protection Regulation (GDPR)

2.1 Referring to paragraph 2.1 of the minutes of the last meeting, the Chairman briefed Members that the PCPD had received 257 enquiries and three complaints concerning the GDPR as of 28 February 2019.

Compliance check against a social media and social networking service company

2.2 Referring to paragraph 3.6 of the minutes of the last meeting, the Chairman briefed Members that according to the information obtained in the compliance check, the company concerned was a US company, which was not bound by the Personal Data (Privacy) Ordinance (the PDPO) as the PDPO lacked extra-territorial jurisdiction. Nevertheless, the company concerned had taken appropriate remedial measures to prevent similar incidents from recurrence.

2.3 Other matters arising from the minutes of the last meeting would be covered in the remaining agenda items of the meeting.

3 Review on the Personal Data (Privacy) Ordinance (Paper No. 02/19)

3.1 The Chairman highlighted the initial views of the Privacy Commissioner for Personal Data (PCPD) on the review of the PDPO to Members; particularly on (i) the threshold for mandatory data breach notification; (ii) the proposed time period for notifying the PCPD; (iii) the proposed timing for notifying the affected persons; (iv) the possible exemptions for notifying affected persons; (v) self-regulation on data retention periods with statutory requirements for specifying maximum retention period; (vi) conferment of sanctioning power on PCPD; and (vii) direct regulation on data processors.
3.2 The Chairman invited Members to express their views on the review of the PDPO and the major views were summarised in the ensuing paragraphs.

Mandatory Breach Notification

3.3 Members generally agreed that mandatory breach notification should be in place and that a higher threshold for breach notification was preferred to a lower threshold. A Member suggested that the organisational data users should be obligated to notify the PCPD, without any exemptions which might apply to notifications to data subjects, for reason that the PCPD would be in the best position to advise whether the organisational data users met the threshold of reporting. The Member also stated that the PCPD should be empowered to direct data users to make notification to affected individuals, when necessary.

3.4 Members also generally agreed that mandatory breach notification should be made to PCPD no later than 72 hours after a reasonable period for the organisations to investigate into suspected data breach coming to their awareness.

Retention Period

3.5 The Chairman briefed Members that Data Protection Principle (DPP) 2 in Schedule 1 to the PDPO should be strengthened such that data subjects would be informed of the maximum retention period on or before collection of personal data of the data subjects under DPP1(3)\(^1\).

3.6 A Member opined that the PDPO should be clear on the retention period. The PCPD might assist specific industries to draw up their retention policies upon request but it would not be appropriate for the PCPD to “dictate” the retention period as most of the profession / businesses have already set their own practices. The Chairman agreed that it would not be appropriate for the PCPD to specify the retention period for industries. Also, there was no such specific statutory requirement in other jurisdictions.

---

\(^1\) DPP1(3) requires all practical steps to be taken by the data user to ensure that the data subject is informed of, amongst other things, whether it is obligatory or voluntary for him to supply the data, the purpose for which the data is to be used, the classes of persons to whom the data may be transferred, on or before the collection of the data.
3.7 Two Members supported the Chairman’s stance and stressed that professions such as doctors might need to retain patients’ personal data for life for valid reason, while consumers may also have expectation on such retention. Hence, it should be up to the market to set their own retention policies.

Sanctioning Power

3.8 The Chairman highlighted that unlike some overseas privacy regulatory authorities such as the Information Commissioner’s Office in the United Kingdom, and other local regulatory bodies such as the Securities and Futures Commission, the Mandatory Provident Fund Schemes Authority and Hong Kong Competition Commission, the PCPD was not vested with any power to impose administrative fines. The PCPD should live up with the worldwide trend, such as the GDPR in imposing severe level of administrative fines, so as to add deterrent effect on data users. This was particular so where a contravention of DPPs is not per se a criminal offence, but only until one failed to comply with the Enforcement Notice. The current thinking was to set the maximum fine level at 3% of local annual turnover, or HK$10 million, whichever is higher.

3.9 A Member added that to reflect the global trend and address the general quest from the society, a more severe level of fine would mean an enhanced regulatory regime in the eyes of the public. The crux hinged on how to ensure that the enforcement could meet the standard and it required building of trust among the public. Another Member asked if the PCPD was conferred the power to levy administrative fines, whether the public would have faith in the PCPD in conducting the whole process of investigation.

3.10 A Member agreed that it would be important to set a reasonable amount of fine and yet it would be a difficult task to set a level which could be described as having sufficient deterrent effect, especially towards multinational organisations. That said, if the PCPD was empowered with the sanctioning power and a certain amount of fine would be imposed in cases of data breach, the aggrieved public would at least felt that their aggrievances were somewhat addressed.

3.11 The Chairman opined that if the PCPD was conferred with the sanctioning power as requested, clear standards and criteria for levying fines as well as a reasonable level of fines should be formulated and the factors to be taken
into account when exercising sanctioning power should be devised. However, the PCPD would not blindly follow the requirement of the GDPR. Local circumstances would have to be emphasised. Some of the factors included the number of the affected individuals, the nature of personal data being leaked, etc. This would enable Hong Kong to be the regional data hub for the Mainland China under “One Country, Two System” and the “Belt and Road Initiative”.

3.12 The Chairman thanked for Members’ views and concurred with the importance of setting a right balance.

Direct Regulation on Data Processors

3.13 The Chairman introduced the idea of having direct regulation on data processors, as opposed to merely regulating data users under the current regime. This would be in addition to the current indirect regulation on data processors by requiring data users to adopt contractual or organisational measures.

3.14 Overall, Members were in general supportive of the various proposals outlined.

4 Consultation on Access to Information and Archives Law (Paper No. 03/19)

Access to Information

4.1 Ms Raina YEUNG, Assistant Privacy Commissioner (Legal, Policy and Research) highlighted the PCPD’s preliminary views on the Access to Information Sub-Committee. The PCPD’s preliminary views mainly focused on selected recommendations in the Consultation Paper on Access to Information (the ATI) that might have implications on personal data privacy protection. In response to whether data which could not be accessed under the PDPO could otherwise be accessed under the proposed ATI regime, and vice versa, a Member replied that it would be unlikely that data inaccessible under PDPO could be accessed under the proposed ATI regime. However, it might be possible that data which could be disclosed under PDPO could not be disclosed under the proposed ATI regime. One of the envisaged situations was appraisal report (such as for employment purpose or giving an honour or award) which contained opinions about another person. The said appraisal
however might be disclosable under the proposed ATI regime since only a qualified exemption applied.

4.2 If the disclosure of the relevant assessment about the individual would inhibit / undermine the frankness and candour of internal discussion on giving an honour or award to an individual, the relevant assessment about the individual should not be disclosed under the proposed ATI regime.

4.3 The Member also clarified that in the proposed ATI regime, if the Ombudsman overturned the internally-reviewed decision of a government department or public body for refusing an ATI request, it would be the government department or public body as opposed to the Ombudsman to disclose the requested information.

4.4 The Member explained the difference between absolute exemption and qualified exemption. In absolute exemption, the public body had no obligation to balance public interest for and against disclosure whereas in qualified exemptions, the public body was imposed with such obligation.

Archives Law

4.5 Ms Raina YEUNG highlighted the PCPD’s preliminary views on archives law. The PCPD’s preliminary views focused on selected consultation questions in the Consultation Paper on Archives Law that might have implications on personal data privacy protection.

4.6 Ms Raina YEUNG briefly mentioned (i) the balance between the preservation of archives and protection of personal data (i.e. in relation to Consultation Question 7 in AL Consultation Paper); (ii) section 63D of the PDPO under which government records being transferred to the Government Records Service for appraising the preservation value would be dispensed with the requirement of DPP 3 (i.e. personal data must not be used for a new purpose unless with the consent of a data subject); and (iii) the retention of census schedules after a census exercise.

4.7 A Member asked if it would be legally in order for a data user to obtain from a data subject consent to the use of personal data for all purposes and for a long period of time. Ms Raina YEUNG replied that if there was an overriding public interest to be served, this could be considered acceptable
as in the context under discussion regarding seeking the consent of data subjects for keeping the census raw data beyond two years. In the commercial context, such practice could amount to waiving of certain obligations of a data user. Conversely, from the perspective of personal data privacy protection, it would tantamount to depriving certain rights of a data subject under the PDPO that would raise privacy concern.

4.8 Another Member expressed her views on retention of census schedules. Raw data from the census schedules might have archival and research value after many years, for example, studying the impact of a disaster or a contagious disease on population growth. However, it was crucial that the data used would not be traced back to the identity of an individual.

4.9 Members generally agreed that redaction of the identity of an individual from the census schedule would be one of the methods to conduct studies using archive records without infringing personal privacy. Another Member gave a remark that redaction and removal of personal data from census schedules would be more feasible in the digital era.

5 Report on PCPD’s major activities (Paper No. 04/19)

5.1 The Chairman highlighted the PCPD’s major activities to the Members.

6 Report on 2018 and 2019 PCPD’s business plans (Paper No. 05/19 & 06/19)

6.1 Upon the Chairman’s invitation, Mr Daniel LEUNG, Chief Personal Data Officer (Head of Corporate Support Division) briefed Members on the implementation of PCPD’s Business Plan 2018. A Member considered that whilst meeting performance target was important, some complicated cases might call for relatively substantial input that would necessitate more time for handling.

6.2 The Chairman also updated Members on the PCPD’s Business Plan 2019.

7 PCPD’s Internal Compliance Check (Paper No. 07/19)

7.1 Mr Daniel LEUNG briefed Members that two minor irregularities identified in the PCPD’s internal compliance check were addressed by speedy remedial
or follow-up actions. PCPD would strive to enhance its internal management and corporate governance.

8 **Any other Business**

*Schedule of next meeting*

8.1 The next meeting was scheduled on 3 July.