

立法會
Legislative Council

Ref : CB2/PL/CA

LC Paper No. CB(2)684/09-10
(These minutes have been seen
by the Administration)

Panel on Constitutional Affairs

**Minutes of special meeting
held on Friday, 11 September 2009, at 3:00 pm
in the Chamber of the Legislative Council Building**

- Members present** :
- Hon TAM Yiu-chung, GBS, JP (Chairman)
 - Ir Dr Hon Raymond HO Chung-tai, SBS, S.B.St.J., JP (Deputy Chairman)
 - Hon Albert HO Chun-yan
 - Dr Hon Margaret NG
 - Hon CHEUNG Man-kwong
 - Hon Mrs Sophie LEUNG LAU Yau-fun, GBS, JP
 - Hon WONG Yung-kan, SBS, JP
 - Hon LAU Kong-wah, JP
 - Hon Miriam LAU Kin-ye, GBS, JP
 - Hon Abraham SHEK Lai-him, SBS, JP
 - Hon Audrey EU Yuet-mee, SC, JP
 - Hon WONG Kwok-hing, MH
 - Hon Jeffrey LAM Kin-fung, SBS, JP
 - Hon LEUNG Kwok-hung
 - Hon CHEUNG Hok-ming, GBS, JP
 - Hon Ronny TONG Ka-wah, SC
 - Hon CHAN Kin-por, JP
 - Dr Hon Priscilla LEUNG Mei-fun
 - Hon CHEUNG Kwok-che
 - Hon IP Kwok-him, GBS, JP
 - Dr Hon PAN Pey-chyou
- Members absent** :
- Dr Hon Philip WONG Yu-hong, GBS
 - Hon LAU Wong-fat, GBM, GBS, JP
 - Hon Emily LAU Wai-hing, JP
 - Hon Timothy FOK Tsun-ting, GBS, JP
 - Hon LI Fung-ying, BBS, JP
 - Hon LEE Wing-tat
 - Hon WONG Ting-kwong, BBS, JP
 - Hon CHIM Pui-chung
 - Prof Hon Patrick LAU Sau-shing, SBS, JP
 - Hon Cyd HO Sau-lan

Dr Hon LAM Tai-fai, BBS, JP
Hon WONG Sing-chi
Hon WONG Kwok-kin, BBS
Hon WONG Yuk-man
Hon IP Wai-ming, MH
Hon Mrs Regina IP LAU Suk-ye, GBS, JP
Dr Hon Samson TAM Wai-ho, JP

- Public Officers attending** : Mr Stephen LAM Sui-lung
Secretary for Constitutional and Mainland Affairs
- Mr Arthur HO Kin-wah
Deputy Secretary for Constitutional and Mainland Affairs
- Miss Joanna CHOI Chuen-han
Principal Assistant Secretary for Constitutional and Mainland Affairs
- Mr Roderick B WOO
Privacy Commissioner for Personal Data
- Miss Brenda KWOK
Acting Deputy Privacy Commissioner for Personal Data
- Mr K T CHAN
Chief Personal Data Officer
- Clerk in attendance** : Miss Flora TAI
Chief Council Secretary (2)3
- Staff in attendance** : Ms Connie FUNG
Senior Assistant Legal Adviser 1
- Ms Clara TAM
Assistant Legal Adviser 9
- Mrs Eleanor CHOW
Senior Council Secretary (2)4
- Mrs Fanny TSANG
Legislative Assistant (2)3
-

Action

I. Consultation Document on Review of the Personal Data (Privacy) Ordinance

[LC Paper Nos. CB(2)2410/08-09(01), CB(2)2445/08-09(01), CB(2)2473/08-09(01) and (02) and Consultation Document on Review of the Personal Data (Privacy) Ordinance]

Secretary for Constitutional and Mainland Affairs (SCMA) briefed members on the Administration's paper which set out the background of the Consultation Document on the Review of the Personal Data (Privacy) Ordinance (PD(P)O) (the Consultation Document) and summarised the major proposals contained therein [LC Paper No. CB(2)2410/08-09(01)]. He said that the Administration was open-minded about the proposals and welcomed the views of the community and Legislative Council (LegCo) Members in this regard.

2. The Privacy Commissioner for Personal Data (the Commissioner) briefed members on the paper provided by the Office of the Privacy Commissioner for Personal Data's (PCPD) on the Consultation Document which set out the background of the review of PD(P)O conducted by the Office, the major proposals put forth by PCPD to amend PD(P)O as well as major areas of difference in views between the Administration and PCPD [LC Paper No. CB(2)2473/08-09(01)]. Members noted that PCPD had also provided an information paper which contained proposals made by PCPD to SCMA and relevant privacy issues [LC Paper No. CB(2)2473/08-09(02)].

3. Members also noted that the LegCo Secretariat had prepared a background brief on "Review of PD(P)O" for the Panel's reference [LC Paper No. CB(2)2445/08-09(01)].

Presentation of the Consultation Document and its proposals

4. Ms Miriam LAU observed that the Consultation Document had set out 12 major proposals which sought to enhance the regulation of personal data, 15 other proposals in Annex 1 which had considerable impact on the community on which comments were invited, and nine proposals in Annex 2 which the Administration was inclined not to pursue. The 12 major proposals could also be grouped into three categories -

- (a) a set of proposals which the Administration had explained in detail the background and justifications for the proposals, such as the measure to enhance the security of sensitive personal data in Proposal No. 1;
- (b) a set of proposals which the Administration had explained why they should not be supported, such as Proposal No. 4 which sought to grant criminal investigation and prosecution power to PCPD; and

Action

- (c) a set of proposals which were put forward notwithstanding the fact that PCPD had not encountered problems in respect of the relevant issues, such as Proposal No. 11 which sought to impose a heavier penalty for repeated non-compliance with enforcement notice.

Ms LAU considered that the presentation of the Consultation Document was obscure. Since no justification was given for the introduction of the proposals referred to in paragraph 4 (b) and (c) above, it would be difficult for members to grasp the merits of these proposals and to consider whether to support them.

5. SCMA explained that the Administration had set out all the relevant proposals and presented them in the Consultation Document with analysis given. The proposals referred to in paragraph 4 (b) and (c) were suggested by PCPD who was in a better position to explain why they should be introduced.

6. The Commissioner said that to facilitate members and the public to better understand its proposals, PCPD had explained in its paper the main proposals and their objectives, as well as the major areas of difference in views between the Administration and PCPD. A large volume of research and reference materials was collected during its review of PD(P)O. To enable the public to have a holistic view of the review exercise conducted since 2006, PCPD had therefore prepared and upload an information paper onto its website which contained all relevant information of the major proposals made by PCPD to the Administration [LC Paper No. CB(2)2473/08-09(02)].

7. On the justifications for proposing the granting of more enforcement power to PCPD, the Commissioner pointed out that PCPD was already performing multifarious duties. Apart from enforcing PD(P)O, PCPD was also responsible for providing education, training and advice on matters relating to personal data privacy, as well as for handling complaints, conducting investigation and acting as mediator in disputes relating to personal data privacy. Acting Deputy Privacy Commissioner for PCPD (Deputy Commissioner) supplemented that Proposal No. 11 was part and parcel of the package of proposals put forth by PCPD to amend PD(P)O with a view to enhancing the protection for personal data privacy. Proposal No. 11 sought to curb against repeated offenders who did not comply with enforcement notices. Although there was no such repeated offence recorded, PCPD believed that prevention was more effective than cure. In addition, the power of PCPD to issue enforcement notice was restricted at present. This might account for the reason why PCPD had not come across repeated non-compliance with an enforcement notice. Proposal No. 20 was made to provide wider discretionary power on PCPD to issue enforcement notices. Given that it was not uncommon for different complainants lodging complaints against the same data user at different times on the same or similar facts, PCPD had thus proposed to step up sanction against repeated offenders.

Action

8. Mr WONG Kwok-hing expressed support for tightening the regulation of personal data with a view to enhancing personal data privacy protection. Referring to the recent personal data leakage cases of the Police Department and the Hospital Authority, he, however, expressed concern whether the proposals put forward in the Consultation Document would enhance the security of personal data collected through government departments. Mr WONG pointed out that given that different types of government employees would participate in the handling of such personal data, including those on pension terms, on non-civil service contract terms, and those hired through employment agencies, etc., there was a risk of abusive use of personal data. Mr WONG also enquired how PCPD would monitor the work of the Government in safeguarding personal data under the proposals put forward in the Consultation Document.

9. SCMA assured members that government bureaux and departments had all along acted in compliance with the spirit and requirements of PD(P)O. They would continue to do so, if any proposed legislative amendments were enacted. Arising from a spate of data leakage incidents in the past two years, the Administration had drawn up internal guidelines and established procedures to deal with data leakage cases. This required bureaux/departments to report the case to PCPD as soon as possible and to notify affected individuals as far as practicable. Government departments concerned had acted in accordance with the guidelines and procedures. SCMA further said that all government staff, irrespective of their terms of employment, were obliged to observe the regulations and instructions promulgated on information security and protection of personal data related to their work. It was also the responsibility of every member of staff to comply with PD(P)O.

10. The Commissioner said that his office was responsible for overseeing the enforcement of PD(P)O in both the private and public sectors. PCPD had investigated the leakage of witness statements in the Police Department and was currently studying the protection of electronic medical data kept by the Hospital Authority.

Enforcement powers of PCPD

11. Mr Ronny TONG enquired why the Administration supported the proposal of conferring on PCPD the power to provide legal assistance to aggrieved data subjects (Proposal No. 5), but did not support the proposal of granting criminal investigation and prosecution power to PCPD (Proposal No. 4).

12. The Commissioner informed the Panel that in its original proposals, PCPD had recommended conferring more power on PCPD so as to step up the protection for personal data privacy right. The Administration, however, had reservations about some of the proposals. PCPD's proposals to confer more power on PCPD included the following -

Action

- (a) the power to conduct criminal investigation and prosecute criminal offence cases;
- (b) the power to provide assistance to aggrieved data subjects in respect of legal proceedings;
- (c) the power to impose monetary penalty on serious contravention of a data protection principle (DPP); and
- (d) the power to award compensation to an aggrieved data subject after conclusion of an investigation.

13. The Deputy Commissioner supplemented that PCPD considered that the Commissioner, who possessed the expertise and first hand information on a case, could act expeditiously to deal with the suspected offence if he was granted the criminal investigation and prosecution power. Granting independent prosecution power to PCPD would also help prevent conflict of interest where the Police or other government departments were involved in the case as data user.

14. SCMA explained the Administration's position on the proposals relating to the enforcement of power of PCPD as follows -

- (a) under the Basic Law, the control of criminal prosecutions was vested in the Department of Justice (DoJ). Although it would not be inconsistent with the Basic Law to confer prosecution power on PCPD if the relevant legislation expressly stated that the prosecutions to be brought thereunder were without prejudice to the powers of the Secretary for Justice in relation to prosecution of criminal offences, the policy assessment was that strong justifications were required for the prerogative of initiating criminal prosecution to be delegated in specific domains;
- (b) under the existing arrangements, the power to conduct criminal investigation, prosecute and give ruling on criminal cases were vested with three separate authorities, namely the Police, DoJ and the Judiciary respectively, in order to ensure a fair trial and judicial independence. The Administration attached great importance to these principles and had reservations about conferring the power of criminal investigation, prosecution and imposing penalty on one single authority;
- (c) the appropriate body to determine compensation under PD(P)O had been thoroughly discussed in the Law Reform Commission (LRC) Report on Reform of the Law Relating to the Protection of Personal Data published in August 1994. LRC opined that conferring power on a data protection authority to award compensation would vest in a

Action

single authority an undesirable combination of enforcement and punitive functions. LRC recommended that PCPD's role should be limited to determining whether there had been a breach of DPPs. It would be for the court to determine the appropriate amount of compensation payable. The Administration shared the same view. The Administration would invite views on whether it was appropriate to introduce an additional redress avenue by empowering PCPD to award compensation to aggrieved data subjects;

- (d) it was not common for non-judicial bodies to have the statutory power to impose monetary penalties. In addition, whether an act constituted a serious contravention of a DPP was a matter of subjective judgment. The Administration would invite views on whether it was appropriate to empower PCPD to impose monetary penalty for serious contravention of DPPs; and
- (e) if PCPD was empowered to offer legal assistance to an aggrieved data subject who suffered damage to seek redress under PD(P)O, the aggrieved party would be in a better position to assess the chance of success of his civil claim and would not be inhibited from filing a lawsuit due to cost considerations. The proposal, if pursued, could achieve greater deterrent effect on acts or practices which intruded into personal data privacy, and enhance the overall effectiveness of sanctions provided for under PD(P)O.

15. Dr Margaret NG said that in creating a new offence, one must abide by the basic legal principle of making specific the offence clear and with full justification in order to prevent injustice. While the enforcement of PD(P)O might not be satisfactory, measures to step up enforcement actions, instead of imposing more penalties, creating criminal offences and conferring more power on the Commissioner, could be an answer to the problem. Dr NG said that she did not support Proposal No. 4 which sought to grant criminal investigation and prosecution power to PCPD. In her view, prosecution power should be vested in an independent body in accordance with the existing constitutional framework. She considered the present arrangement to empower executive departments such as the Customs and Excise Department and the Immigration Department with prosecution power not satisfactory. She pointed out that as PCPD was the enforcer of PD(P)O, the proposal to confer criminal investigation and prosecution power on PCPD would give rise to conflict of interests. She added that she was not convinced of the need to create criminal offences after having considered the information and analysis given in the Consultation Document.

Action

16. The Commissioner responded that the proposal to confer prosecution power on PCPD was formulated taking into account the views of some members of the Panel on Information Technology and Broadcasting (ITB) expressed earlier. PCPD was open-minded about the proposal and appreciated dissenting viewpoints expressed by members.

17. SCMA said that he agreed with the viewpoints expressed by Dr NG on enforcement power of PCPD. As regards creating new criminal offences, the Administration was aware of the need to give specific and clear legislative intent in its proposals and to set a higher threshold for criminalising certain acts. On measures to step up enforcement, Proposal No. 5 proposed to provide legal assistance to an aggrieved data subject so that he or she would have the means to file a lawsuit when the case warranted it, and Proposal No. 40 proposed to extend the time limit for laying information for prosecution of an offence under PD(P)O.

Proposal No. 8 : Unauthorized Obtaining, Disclosure and Sale of Personal Data

18. Mr WONG Kwok-hing expressed concern about the misuse and unauthorised use of personal data on the Internet which had aroused widespread public concern. He enquired whether any of the proposals in the Consultation Document would address the problem and hold the disseminator culpable for leakage of such data.

19. SCMA responded that given that unauthorised use of personal data might intrude into personal data privacy and might cause damage to data subjects, Proposal No. 8 suggested making it an offence if a person obtained personal data without the consent of the data user and disclosed the personal data so obtained for profits or malicious purposes.

20. The Commissioner said that while Proposal No. 8 sought to address the problem of unauthorised leakage of personal information, whether it could achieve that effect would depend on the amendment to be passed by LegCo. The role of PCPD was to monitor the compliance with PD(P)O by the Government and the public.

21. Mr IP Kwok-him enquired about the definition of "malicious" purposes and expressed concern that members of the public might be trapped to commit the offence inadvertently if the definition was not clear. He said that the proposal should strike a balance between personal data protection and the right to access information as well as freedom of expression.

22. SCMA explained that Proposal No. 8 sought to protect data subjects whose personal data were leaked and to deter irresponsible acts of those who obtained or disclosed such leaked data without the consent of the data user, which seriously intruded into the personal data privacy of the data subject concerned. The proposal did not seek to impose criminal liabilities on data users for accidental

Action

leakage of personal data not resulting in substantial harm. The proposal was couched in specific terms in order not to catch those who had disseminated personal data unintentionally. Several issues needed to be further deliberated if the proposed offence was to be implemented, for example, whether a person with a reasonable defence should not be held liable.

23. Mr Ronny TONG was of the view that PD(P)O should be reviewed and overhauled given its deficiencies as reflected in a series of personal data leakage cases in the past few years. He, however, queried the effectiveness of Proposal No. 8 and enquired why the Administration had not considered imposing civil liabilities, instead of criminal liabilities, on persons leaking personal data. He said that civil remedies included, among others, the issue of an injunction order which would help prevent further dissemination of personal data. Through civil proceedings, a data subject could claim damages or even obtain an account of profit from the data user who had disclosed personal data for profits purposes.

24. The Commissioner said that the breach of any of the six DPPs stipulated in Schedule 1 to PD(P)O did not constitute a criminal offence. However, section 66 of PD(P)O already provided a civil remedy to any person who suffered damage including injury to feelings by reason of a contravention of a requirement under PD(P)O to seek compensation from the data user.

25. SCMA responded that under the existing law, a data subject who suffered damage by reason of a contravention of a requirement under PD(P)O was given the opportunity to seek compensation from the data user for that damage. In order to create greater deterrent effect on acts or practices which intruded into personal data privacy and to enhance the overall effectiveness of sanctions provided for under PD(P)O, Proposal No. 5 further suggested conferring on PCPD the power to provide legal assistance to aggrieved data subjects. With the provision of legal assistance, an aggrieved party would then not be inhibited from filing a lawsuit due to cost considerations.

26. Mr Ronny TONG said that it was difficult to assess the damage in monetary terms when claiming compensation for personal data leakage. He therefore had proposed that application for a court order should be made to stop further dissemination of personal data when leakage arose. Nevertheless, he supported the proposal to provide legal assistance to data subjects when warranted.

27. SCMA responded that the Administration would consider providing the Commissioner with more resources if Proposal No. 5 was to be pursued. The Administration would consider the views given by Mr TONG.

28. Dr Priscilla LEUNG enquired whether legal liability would be imposed on a third party who had intruded into personal data privacy and caused damage to a data subject by disseminating his/her personal data on the Internet.

Action

29. The Deputy Commissioner responded that PCPD had proposed to address the problem by -

- (a) creating a new offence for unauthorised obtaining, disclosure and sale of personal data without the consent of the data user; and
- (b) adding a new definition of "sensitive personal data" and making new provisions prohibiting the collection, holding, processing and use of sensitive personal data except with the consent of the data subject.

30. SCMA said that if Proposal No. 8 was implemented, irresponsible dissemination of leaked personal data for profits or malicious purposes and without the consent of the data user would be an offence. As regards sensitive personal data, the Administration had an open mind and would welcome public views as to whether biometric data such as iris characteristics, hand contour reading and fingerprints should be classified as sensitive personal data. Some overseas jurisdictions classified other personal data such as political affiliation, religious beliefs and sexual orientation as sensitive personal data. The Administration considered that it would be controversial to define these personal data as sensitive personal data. Moreover, the media in Hong Kong often gathered such personal data of celebrities for reporting purpose. In order not to hinder the freedom of expression, the Administration was inclined not to define personal data of this kind as sensitive personal data. However, the Administration would listen to the public views during the consultation period before putting forward any legislative proposals.

31. The Commissioner, however, expressed concern that Proposal No. 8 of criminalising the act of disclosing data for profits or malicious purposes could not plug the loophole of the existing legal framework. Under the existing legislation, exemption from PD(P)O was given to personal data held by an individual for domestic or recreational purposes. In a recent case, a Taxation Officer of the Inland Revenue Department who had recorded the personal particulars of 13 400 taxpayers for his personal future use was acquitted from the charge of misconduct in public office because the prosecution could not prove that his collection of taxpayers' personal data was intended for profits or malicious use.

Proposal No. 14 : Parents' Right to Access Personal Data of Minors

Proposal No. 27 : Transfer of Personal Data of Minors Relevant to Parental Care and Guardianship

32. Dr Priscilla LEUNG expressed concern about the negative approach adopted for formulating Proposal Nos. 14 and 27 which had projected a negative image of parents. She considered that the proposals which sought to restrict parents' right to access personal data of minors were premised on the assumption that many parents were irresponsible and they might abuse the data access mechanism to obtain the personal data of the child for the parents' own purpose

Action

rather than for the interests of the child. Dr LEUNG believed that the majority of parents took good care of their children and the proposals set out in the Consultation Document should be premised on the understanding that most parents would access personal data of children for the purpose of protecting the well-being of children, such as to communicate effectively with teachers and doctors, rather than the other way round. She expressed concern about parents being restricted from accessing personal data of minors who were very young, say six years old, and the right of a social worker to decline parents' request for access to personal data of the child. Dr LEUNG considered that the court was the only appropriate avenue to decide whether a request for access to a child's personal data made by his/her parent was reasonable.

33. SCMA responded that the concerns raised by Dr LEUNG were envisaged by the Administration. The Administration considered that any proposal to restrict parents' right to their children's personal data was controversial, as it touched on the sensitive issues of the rights and obligations of parents in caring for their children. It was therefore important to strike a balance between respecting parents' right to have reasonable access to the personal data of their children and respecting the children's privacy right. Proposal Nos. 14 and 27 as set out in Annex 1 to the Consultation Documents would have considerable impact on the community and the Administration would like to collect more views from the public. SCMA added that Proposal No. 14 was put forward on the basis of the recommendation made by PCPD (equivalent to Proposal No. 20 in the Annex to PCPD's information paper).

34. The Commissioner explained that by virtue of section 18(1) of PD(P)O, a parent had the right to make a request on behalf of his/her child to access the child's personal data. Proposal No. 14 sought to address exceptional cases where the child had expressed to the data user his/her disagreement to the disclosure of his/her personal data to his/her parents. The proposal was formulated having regard to the concerns raised by some social workers who had been faced with the dilemma of whether or not to accede to parents' data access request to disclose the child's personal information confided in them. The proposal sought to provide a ground of refusal that a social worker might exercise if disclosure of the child's personal data to the parent would not be in the best interests of the child. He said that PCPD was open-minded about the proposal and welcomed public's comments.

Internet Protocol Address as Personal Data

35. Mr Albert HO referred to the Yahoo's case in 2005 in which Yahoo! Holdings (Hong Kong) Limited had disclosed user information corresponding to an Internet Protocol (IP) address of a journalist who was an email user of Yahoo! China residing in the People's Republic of China (PRC), leading to his arrest and conviction of the crime of illegally providing state secrets to foreign entities outside PRC. Mr HO expressed disappointment that the Administrative Appeals Board (AAB), which investigated the complaint lodged against the email service

Action

provider for infringing the provisions of PD(P)O by disclosure of an email subscriber's personal data, concluded that the IP address and the log-in information of the subscriber's e-mail account did not constitute personal data within the definition of PD(P)O. Mr HO considered that applying such a restrictive interpretation of the term "personal data" defined in PD(P)O and the transfer of personal data from Hong Kong to another jurisdiction which did not have comparable personal data protection system had tarnished the reputation of Hong Kong. He questioned whether it was reasonable for Hong Kong to provide personal data to an overseas jurisdiction for the purposes of prevention or detection of crime, if the criminal proceedings of the jurisdiction concerned were operated under a different regime. He expressed concern that if the Administration continued to adopt a conservative approach and did not review the scope of the application of PD(P)O, the power of IP providers to disclose personal data of their subscribers and to pass intelligence to another authority would be unchecked, which would infringe the personal data privacy of data subjects.

36. The Commissioner recalled that when he discussed the Yahoo's case with members of the ITB Panel in 2005, he had expressed the view that the IP address per se might not amount to "personal data" as defined under PD(P)O and hence PCPD could not conduct an investigation on the case. AAB had subsequently affirmed that view. Having regard to the Yahoo's case, PCPD had suggested to the Administration -

- (a) to review whether IP address should be regarded as "personal data" within the definition of PD(P)O;
- (b) to consider whether the collection and use of personal data outside Hong Kong by a data user in Hong Kong should be regulated by PD(P)O; and
- (c) to consult the public on the definition of "crime" under the section 58 exemption provisions of PD(P)O.

37. SCMA said that as far as the Yahoo's case was concerned, PCPD had discharged its duties in accordance with PD(P)O. The Administration had reservations about deeming IP address per se as "personal data" and its views were set out in paragraphs 7 to 10 of Annex 2 to the Consultation Document. In gist, deeming IP address per se as personal data would place an unreasonable burden on and pose serious compliance problems to various industry players in the information technology industry. There was a need to strike a balance between protection of personal data privacy and normal business operation.

Action

Section 33 of PD(P)O

38. Noting that section 33 of PD(P)O, which stipulated that data users in Hong Kong were prohibited from transferring data to another territory where comparable privacy protection was lacking, was the only provision which had not commenced operation, Mr IP Kwok-him enquired why the Consultation Document was silent on the issue. He also enquired about the reason for not implementing section 33 and whether the provision needed to be reviewed.

39. SCMA said that he was aware that PCPD had taken some time to consider how to implement section 33. Under the provision, one of the permitted circumstances for transfer of personal data outside Hong Kong was that the place to receive the personal data had in place an acceptable data protection regime. Commencement of section 33 necessitated PCPD to specify places with law substantially similar to, or served the same purposes as PD(P)O. The Commissioner said that PCPD was ready to implement section 33, pending the Administration's decision.

Application of PD(P)O to offices set up by the Central People's Government (CPG) in the Hong Kong Special Administrative Region (HKSAR)

40. Mr LEUNG Kwok-hung said that section 18(1) of PD(P)O provided that an individual might make a request to be informed by a data user whether the data user held personal data of which the individual was the data subject. He suspected that the Liaison Office of CPG in HKSAR was holding his personal data and enquired about the applicability of PD(P)O to CPG offices set up in HKSAR.

41. SCMA responded that the purpose of this meeting was to discuss the review of PD(P)O. He affirmed that PD(P)O was applicable to the HKSAR Government. The issue of whether and, if so, how PD(P)O should apply to CPG offices set up in HKSAR would be dealt with in a different context, i.e. the adaptation of laws exercise.

II. Any other business

42. The Chairman informed members that the next meeting of the Panel would be held on 15 October 2009 to elect chairman and deputy chairman of the Panel for the 2009-2010 legislative session. Briefing to the Panel on the 2009-2010 policy initiatives relating to constitutional, mainland and human rights matters would be held on 19 October 2009.

43. The meeting ended at 4:37 pm.