PCPD's Submission in response to the

Consultation Paper on

Real-name Registration for SIM Cards

This submission is made by the Office of the Privacy Commissioner for Personal Data ("**PCPD**") in response to the Consultation Paper published by the Commerce and Economic Development Bureau in January 2021 on the proposed real-name registration programme for subscriber identity module ("**SIM**") cards (the "**Proposed Programme**").

2. Under the Proposed Programme, all mobile telecommunication service subscribers[1] will be required to register their names and certain personal particulars[2]. The purpose is apparently to facilitate crime prevention and detection by making it easier for the law enforcement agencies to trace criminals who otherwise could take advantage of the anonymous nature of pre-paid SIM cards to pursue illegal activities.

3. As an independent body established to monitor and enforce compliance with the Personal Data (Privacy) Ordinance (Cap.486) ("**PDPO**"), the PCPD offers observations on the Proposed Programme from the perspective of the protection of personal data privacy.

Compliance with the Requirements of the PDPO

4. Under the Proposed Programme, service operators[3] will be responsible for the collection, holding, processing and use of personal data provided by subscribers. The importance that the service operators will have to comply with the requirements of the

[1] The term "subscriber" used in this submission has the same meaning as the term "user" in the Consultation Paper.

[2] Currently subscribers of pre-paid SIM cards simply purchase SIM cards from vendors and do not have to provide any personal particulars. Those using SIM service plans provide certain personal particulars as required under their contracts with the service operators.

[3] The term "service operator" used in this submission has the same meaning as the terms "operator /mobile service providers", as well as "licensees" where appropriate, in the Consultation Paper.

PDPO, including the Data Protection Principles ("**DPP**" or "**DPPs**") therein[4] as regards the collection, holding, processing and use of personal data cannot be over-emphasized. In the ensuing paragraphs we would like to point out matters which are considered to be of particular relevance.

Data collection

5. Under the Proposed Programme SIM card subscribers will need to provide the following information to the service operators for registration[5]:

(a) name;

(b) identity document number;

(c) copy of the identity document; and

(d) date of birth.

6. Instead of the current practice that subscribers of SIM service plans provide their personal data to the service operators face-to-face, other means of registration, such as self-registration facilitated online or through mobile apps, will be feasible insofar as pre-paid SIM card subscribers are concerned. The mobile services will be activated after the service operators have received and verified the data provided by the subscribers.

7. The types of information set out in paragraph 5 above are personal data[6] of the SIM card subscribers (being data subjects[7]).

---

[4] Paragraph 3.9 of the Consultation Paper.

[5] Paragraph 3.3 of the Consultation Paper. If the subscriber is a company the required information will have to be provided in respect of the person designated by the company for registration purpose (paragraph 3.5 of the Consultation Paper). If the subscriber is below the age of 16 the required data will have to be provided in respect of the "appropriate adult" named for the purpose (paragraph 3.7 of the Consultation Paper).

[6] "Personal data", as defined in section 2(1) of the PDPO, means "*any data* –
(a) relating directly or indirectly to a living individual;
(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
(c) in a form in which access to or processing of the data is practicable."

[7] A "data subject" means an individual who is the subject of the data, as defined in section 2(1) of the PDPO.

8. Pursuant to DPP1 of the PDPO, personal data should only be collected if it is[8]:

(a) collected for a lawful purpose directly related to a function or activity of the data users;

(b) necessary for or directly related to the purpose(s) of collection; and

(c) adequate but not excessive in relation to the purpose(s) of the collection.

In addition, personal data shall be collected by means which are lawful and fair in the circumstances of the case[9].

9. For the Proposed Programme the purposes of collecting subscribers' personal data appear to be (1) for the operational need of the service operators (such as charging, contract administration, and re-issuing SIM cards in cases of loss or damage) and (2) for tracing the subscribers for crime prevention and detection in appropriate circumstances.

Copy of identity document

10. While collecting the subscriber's name, identity document number and date of birth appears to be reasonably necessary for the said purposes, the need for a copy of the identity document (HKID card in the vast majority of cases) appears to serve the purpose of verifying the personal data provided. It is noteworthy that under DPP 2(1), all practicable steps shall be taken by a data user to ensure that personal data is accurate having regard to the purpose(s) for which the personal data is or is to be used. In the case of application for mobile service it is incumbent upon the service operators to ensure the accuracy of personal data provided by subscribers. By this cases of "identity theft" or related crimes or improper activities could be sieved out or prevented. Service operators will have to provide appropriate instructions and training to their staff for such purpose.

[8] DPP 1(1) (a), (b) and (c), Schedule 1 to the PDPO.

[9] DPP 1(2), Schedule 1 to the PDPO.

11. Given that identity document contains a lot of sensitive personal data, and subject to operational feasibilities, we would suggest that SIM card subscribers should be given an option:

(a) They may choose to register online, and in such a case they would have to provide a copy of the identity document for verification purpose; or

(b) They may choose to register in person at the service operators' offices or shops, and in such a case they would only have to produce the original identity document for verification by the staff, but do not have to provide a copy for retention.

12. The above suggestion would be a less privacy-intrusive measure in that subscribers could choose whether to deposit copies of their identity documents with the service operators.

Data retention duration

13. The Consultation Paper says that subscribers' personal data will be kept for "*at least 12 months*" after the SIM cards are deregistered. The proposed duration is to ensure that perpetrators who have committed crimes would not become untraceable even if they deactivate and destroy the SIM cards[10].

14. DPP2(2) and section 26 of the PDPO stipulate that personal data shall not be kept for a period longer than is necessary for the fulfilment of the purposes for which the data is to be used. To better fulfil the said requirements it is proposed that a definite duration (say, not more than 12 months) should be prescribed for the retention of personal data. A proviso could be added that where crime investigation or prosecution is still ongoing in a particular case the personal data will be erased when the investigation and related actions are completed. In light of the heightened public

[10] Paragraph 3.10 of the Consultation Paper.

expectation on data protection, the Government may wish to explain to the public as to why the proposed duration and the arrangements under the proviso are reasonable and justified in the circumstances.

Use of data for investigation or prevention of crimes

15. The Consultation Paper proposes that law enforcement agencies ("**LEAs**") should be able to request service operators to provide to them SIM card registration records for dealing with urgent or emergency situations on the authorisation of an officer not below the rank of Superintendent[11]. As could be gathered from media reports, this is a matter of concern to the public.

16. We would observe that provisions for similar purposes are included under the PDPO. Section 58(2) provides for an exemption to DPP 3 (regarding use of personal data) whereby data users (service operators in the present context) may disclose personal data of data subjects (subscribers in the present context) to LEAs for the purpose of, among others, preventing or detecting crime.

17. For the sake of legal certainty and affording procedural safeguard against improper disclosure of personal data, we would suggest that, should the Government decide to proceed with the said proposal, consideration may be given to : -

(a) Spelling out clearly under what circumstances the LEAs can request for the registration records which, as could be gathered from the Consultation Paper, would include the following[12]:

(i) for the prevention or detection of crime;

(ii) there is reasonable ground for suspecting that a serious offence has been, or is being, or is about to be committed;

[11] Paragraph 3.14 of the Consultation Paper.

[12] Paragraph 3.14 of the Consultation Paper.

(iii) the nature of the crimes involved is such that swift enforcement actions need to be taken;

(iv) when applying for a magistrate's warrant would cause undue delay resulting in loss or destruction of evidence and hence is impracticable; and

(b) Providing also that the authorising officer's authorisation should be in writing.

The inclusion of the conditions as mentioned in sub-paragraphs (a) and (b) will also help allay public concern about whether subscribers' personal data will be disclosed to LEAs indiscriminately.

Data security

18. Under the Proposed Programme the collected personal data of SIM card subscribers will be kept and stored by the respective service operators and they will be required to establish systems/database to register and safe keep the data[13].

19. In this regard, DPP 4, which provides as follows, should be strictly observed: -

"(1) All practicable steps shall be taken to ensure that any personal data … held by a data user is protected against unauthorized or accidental access, processing , erasure, loss or use having particular regard to –

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data is stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data ; and

(e) any measures taken for ensuring the secure transmission of the data."

[13] Paragraph 3.8 of the Consultation Paper.

It would help allay public concerns for the public to be advised of the details of the systems when they are available.

20. It would be desirable from a data security perspective if the Communications Authority, who will be issuing guidelines concerning the running of the Proposed Programme, also sets out in detail the technical security measures required. This could include, for instance, (a) developing policies and procedures for regular review of the systems/database, (b) proper access control defining who can access the personal data stored in the systems/database, and (c) taking robust security measures and steps for system login, data transmission and storage.

21. In this connection we would also suggest that the Communications Authority regularly carry out inspections of the systems/database used by the service operators to ensure that adequate data security measures have been put in place. Pursuant to section 7J of the Telecommunications Ordinance (Cap. 106), the Communications Authority may, on giving reasonable prior written notice to a licensee, enter and inspect the offices, premises and places in Hong Kong where the licensee has installed a facility (including equipment associated with the facility), or used for providing services, to verify that the licensee is complying with the licence conditions.

Openness and transparency

22. By virtue of DPP5 service operators will have to take all practicable steps to ensure openness and transparency of their personal data policies and practices. This could be achieved by formulating a Privacy Policy Statement ("**PPS**") setting out the service operator' privacy policies and practices in relation to the personal data it handles (e.g. data retention policy, data security measures and data breach handling mechanism). A PPS should be made available to anyone, in an easily accessible manner, no matter whether personal data is collected by the service operator face-to-face or through mobile apps. Practical guidance in this connection is provided in the publication "*Guidance on*

Personal Information Collection Statement and Privacy Policy Statement" issued by the PCPD[14].

Data access and correction

23. Service providers have to note that by virtue of DPP6 (and sections 18 and 22 of the PDPO) SIM card subscribers are entitled to request access to and correction of their own personal data. Appropriate arrangements have to be made by service operators for such purpose. Practical guidance in this connection is provided in the publications *"Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users"*[15] and *"Proper Handling of Data Correction Request by Data Users"* issued by the PCPD [16].

Sanctions and Compliance

24. It is noted that, pursuant to section 36C (1) of the Telecommunications Ordinance, the Communications Authority is given power to impose financial penalties on licensees for breach of a licence condition, any provision of the Telecommunications Ordinance or its regulation, or the Communications Authority's direction. With a view to providing sufficient deterrent effect, we would suggest that the Communications Authority makes use of its power under the Telecommunications Ordinance to impose financial penalties on service operators who fail to observe the relevant requirements under the Proposed Programme. For instance, they could be required as one of the licence conditions to have regard to the data security requirements set out in the guidelines to be promulgated by the Communications Authority, failing which financial penalties may be imposed.

[14] The publication can be accessed at https://www.pcpd.org.hk/english/publications/files/GN_picspps_e.pdf.

[15] The publication can be accessed at https://www.pcpd.org.hk//english/resources_centre/publications/files/dar2020_e.pdf.

[16] The publication can be accessed at https://www.pcpd.org.hk//english/resources_centre/publications/files/dcr_e.pdf.

Concluding Remarks

25. The views contained in this submission are given without prejudice to the performance of the functions or exercise of the powers of the Privacy Commissioner for Personal Data under the PDPO.

Office of the Privacy Commissioner for Personal Data, Hong Kong

17 March 2021