Comments on Public Consultation on Review of the Personal Data Protection Act 2012 - Proposed Data Portability and Data Innovation Provisions (Issued 22 May 2019)

Authors

Kow Fangjie, Joshua[1]

Hang Ying Yao[2]

Victor Looi Yi En[3]

All opinions and comments contained in this submission are the personal views of the authors only, and do not reflect the views of the authors' respective employers.

Submitted to: corporate@pdpc.gov.sg

[1] LL.B. (Second Class Upper Honours) (NUS), CIPP/A, CIPM.
[2] LL.B. (First Class Honours) (NUS), LL.M. (Boston).
[3] LL.B. (SMU), B.B.M. (Finance) (SMU).

Introduction

1. The authors of this submission ("**we**", "**our**" and "**us**") thank the Personal Data Protection Commission ("**PDPC**") for the opportunity to provide our opinions and comments on the *Public Consultation on Review of the Personal Data Protection Act 2012 - Proposed Data Portability and Data Innovation Provisions (Issued 22 May 2019)* ("**DPDI Consultation**").

2. By way of background, we are personal friends with a specialised interest in data privacy and information security issues. All opinions and comments contained in our submission are personal to us, and do not reflect the views of our respective employers.

3. All terms used in this response and not otherwise defined herein shall have the meanings ascribed to them in the DPDI Consultation.

Table of Contents

Q2. What are your views on the proposed Data Portability Obligation, specifically (a) scope of organisations covered; and (b) scope of data covered?

4. We generally agree with the imposition of the proposed Data Portability Obligation in Singapore. Nevertheless, we are of the view that:

   (a) Data held in non-electronic forms should also be covered under the scope of the proposed Data Portability Obligation;[4] and

   (b) The requesting individual should be responsible for obtaining all necessary third party consent in connection with a data portability request.[5]

Data held in non-electronic forms should also be covered under the scope of the proposed Data Portability Obligation

5. Paragraph 2.22 of the DPDI Consultation states that the proposed Data Portability Obligation would:

> "*...apply only to data in the possession or control of organisations that is held in electronic form. This is regardless of whether it was originally collected in electronic or non-electronic form. Data held in non-electronic form will not be subject to the proposed Data Portability Obligation. This takes into consideration that imposing the Data Portability Obligation for non-electronic records would entail significant compliance costs for organisations, especially for SMEs that hold data in non-electronic form. Limiting the Data Portability Obligation to data held in electronic form also helps address organisations' concerns regarding compliance costs while ensuring data portability delivers the relevant impact and economic value for Singapore.*" (emphasis added)

6. First, excluding data stored in non-electronic forms from the scope of the Data Portability Obligation may incentivise organisations to avoid upgrading from analog to electronic systems altogether. Many organisations may choose not to store data in electronic forms simply because there is no need to "fix what is not broken". The existence of other pressing business priorities and/or the short-term pain associated with digitalisation are common justifications for many traditional businesses, including law practices,[6] to avoid digitisation of records.

7. By excluding data stored in non-electronic forms, organisations are further incentivised not to upgrade legacy systems or to adopt digital content management systems, as

[4] DPDI Consultation, at para 2.22.
[5] DPDI Consultation, at paras 2.19 - 2.20.
[6] Alfred Chua, "The Big Read: Rise of the machine — how technology is disrupting Singapore's law firms" *Today (19 January 2019), online: Today Online*, where Denton Rodyk's innovation and knowledge management solutions manager Rocio Perez observed that: "*...unless a problem or opportunity — such as one that is related to technological adoption — is of "high-enough priority", an organisation will rarely want to endure the "growing pains that accompany change*".

doing so would subject them to more regulatory obligations in the form of data portability requests. If the PDPC envisions data portability as a means of overcoming analysis in data silos and barriers,[7] then carving out an exception for data held in non-electronic forms detracts from that purpose.

8. Second, excluding data stored in non-electronic forms creates a convenient exception for organisations seeking to artificially limit what they wish to share with a receiving organisation. Notably, paragraph 2.22 states that portability obligations "*apply only to data [...] held in electronic form. This is regardless of whether it was originally collected in electronic or non-electronic form.*"

9. For example, taken literally, valuable data about an individual's meal preferences originally collected by an organisation through an online webform can effectively be shielded from a receiving competitor organisation by printing the forms in hard-copy, erasing the data stored in electronic form when a request is made, and/or subsequently converting such hard-copy forms back into electronic records through manual scanning and optical character recognition technology.

10. Third, we respectfully disagree with the PDPC's consideration that "*significant compliance costs, especially for SMEs*" should deter the imposition of data portability requirements on data held in non-electronic forms. In our view, it is possible for organisations (including SMEs) to transfer compliance costs to the requesting individual by means of a reasonable fee for services provided to the requesting individual to enable organisations to respond to the requesting individual.[8]

11. Allowing a reasonable fee to be charged places the onus on the requesting individual to make astute choices on data portability, requiring the requesting individual to personally evaluate the usefulness of a data portability request against its costs. Valid concerns around exorbitant fees may be alleviated by providing the PDPC with statutory power to review fees for data portability requests, similar to the current mechanism for access and correction requests.[9]

12. Alternatively, the PDPC may provide guidance through publication of written advisory guidelines,[10] or by encouraging the development of industry-specific standards and fee tables. SMEs tend to be the greatest beneficiaries of business digitalisation[11] and "SME status" should not, in our opinion, be used as a shield to deflect validly-made requests

---

[7] DPDI Consultation, at para 2.5.

[8] See, for example, the equivalent mechanism for access requests provided under Regulation 7(1) of the Personal Data Protection Regulations 2014 (No. S 362) ("**PDPR**").

[9] PDPA, at s. 28(1)(b).

[10] PDPA, at s. 49(1).

[11] Janice Heng (roundtable moderator), "Going digital a necessity, not a choice, for SMEs" *The Business Times* (22 May 2018), online: *Business Times*, where panellist Chew Mok Lee notes: "*Digitalisation drives capability and growth, enabling SMEs to stay relevant and become more competitive. Going digital has two key benefits - it makes internal processes more efficient or productive, and companies can capture global opportunities through new channels. For example, a heartland merchant can make informed business decisions and smoothen processes with the implementation of point-of-sales or inventory management systems.*" (emphasis added)

from individuals seeking to port their data to another equivalent provider when compliance costs can be allocated to these individuals.

The requesting individual should be responsible for obtaining all necessary third party consent in connection with a portability request

13. Paragraph 2.31 of the DPDI rightfully recognises that the scope of a data portability request:

> "*... may include personal data of third parties, so long as it was provided by the requesting individual, or generated by the individual's activities. Examples include personal data of the individual's travelling companions provided for a flight booking, and contact lists and photographs which contain personal data of third parties uploaded by the individual to his social media account.*" (emphasis added)

14. However, paragraph 2.32 of the DPDI goes on to state that:

> *"... the porting of such personal data of third parties is unlikely to have any adverse impact on the third parties if the receiving organisation provides for adequate protection of the personal data. The processing of such personal data of third parties by the receiving organisation would only be allowed to the extent that the data is under the control of the requesting individual and used only for that individual's own personal or domestic purposes. The receiving organisation must not use such personal data of third parties for other purposes (e.g. marketing) without the third parties' consent. Consent must be obtained from the third parties involved to collect, use or disclose their personal data for the receiving organisation's other purposes.*" (emphasis added)

15. We are of the view that paragraph 2.32 deserves a relook, as it purports to provide an avenue to disclose third party personal data without the need for consent.[12]

16. First, we wish to point out that "porting" data from one organisation to another falls squarely within the meaning of "disclosure" of personal data by the porting organisation, and "collection"[13] of personal data by the receiving organisation, under the PDPA. Section 13 of the PDPA states in no uncertain terms that organisations shall not disclose or collect personal data unless:

> "*(a) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or*

[12] *Spring College International Pte. Ltd.* [2018] SGPDPC 15, per Deputy Commissioner Yeong at [10], stating that the PDPA adopts a "*... consent-first regime. Unless an exception to consent applies, individual's consent has to be sought.*".

[13] See also, DPDI Consultation at para 2.39, stating that "*[p]orted data that is accepted by the recipient organisation constitutes a collection of personal data by the recipient organisation and is subject to the PDPA or other laws where applicable.*"

(b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law." (emphasis added)

17. The statement that "*porting of such personal data of third parties is unlikely to have any adverse* impact *on the third parties if the receiving organisation provides for adequate protection of the personal data*" is conceptually problematic, as protection[14] is a consideration which is wholly-separate from that of consent.[15] While protection focuses on appropriate arrangements and measures an organisation should take based on a risk assessment,[16] consent centres primarily around the rights of the individual to whom the personal data relates. The implementation of greater security arrangements, in our opinion, does not resolve the fact that consent had not been sought in the first place. Unless the PDPC is of the view that data portability requests fall within Section 13(b), we are of the view that third parties must give, or be deemed to give, their consent for their personal data to be ported from one organisation to another.

18. We are therefore of the view that, in principle, third parties whose personal data is collected and/or transferred in connection with a data portability request must give their consent before the fulfilment of the data portability request. This is also consistent with paragraph 2.39 of the DPDI Consultation, which states that "[p]orted data that is accepted by the recipient organisation constitutes a collection of personal data by the recipient organisation and is subject to the PDPA or other laws where applicable."

19. Furthermore, the requesting individual (as opposed to the receiving organisation) is better placed to obtain such consent from the necessary third parties. In paragraph 2.31 of the DPDI Consultation, two examples are used:

    (a) Individual's travelling companions provided for a flight booking;

    (b) Contact lists and photographs which contain personal data of third parties uploaded by the individual to his social media account.

20. In both examples, it is clear that the requesting individual is in the best position to obtain the consent from the relevant third parties. The requesting individual knows, on a personal level, his travel companions and the details of the third parties in his contact lists and photographs, and may have means of contacting them which are not available to or otherwise not known to either the porting or receiving organisation (e.g. the third party's personal phone number, which is not known to the flight booking company or social media platform).

21. We invite the PDPC to consider other means of placing the onus on the requesting individual, instead of the relevant organisations, to obtain the necessary third party consent in connection with data portability requests.

---

[14] As it is understood under the PDPA, s. 24.

[15] As it is understood under the PDPA, ss. 13 - 17.

[16] PDPC, Advisory Guidelines on Key Concepts in the PDPA (revised 27 July 2017) ("**Key Concepts Guidelines**"), at paras 17.2 - 17.4.

Q4. What are your views on the proposed requirements for handling data portability requests?

22. We agree with the general approach to handling data portability requests as expressed in the DPDI Consultation. We provide our opinions and comments to paragraphs 2.37(a), 2.37(c), and 2.37(d)(i) of the DPDI below:

Paragraph 2.37(a) - Requiring at least one (1) non-electronic avenue for submission of a data portability request.

23. Paragraph 2.37(a) of the DPDI Consultation states that an organisation: "*must provide an avenue for individuals to submit requests for data porting, such as through its website, sending an* electronic *mail to the organisation, or submitting an electronic request via the receiving organisation.*" (emphasis added)

24. We agree with the PDPC's approach here. However, we suggest that this requirement be amended to include at least one physical, non-electronic means of submitting a data portability request for the benefit of less technology-savvy individuals. We note that there may be individuals who are unable to adequately grasp the use of technologically-assisted means to request for services, but nevertheless have a need to port data from one organisation to another. This would include, for example, elderly retirees who wish to switch from one telecommunications service provider to another, but nevertheless wish to retain certain settings or preferences from the previous telecommunications service provider. These individuals may not be savvy enough to submit a data portability request online.

25. Physical, non-electronics means within our contemplation include, but are not limited to, making the request in person at designated locations (e.g. branch offices across Singapore), or by sending a template letter to a physical address, such as the organisation's registered office. We further suggest that a non-exhaustive list of such venues may be provided by the PDPC through written advisory guidelines.

Paragraph 2.37(c) - Individuals should be allowed to view all data to be ported as a starting point

26. Paragraph 2.37(c) of the DPDI Consultation states that: "*[b]efore the organisation ports the data,* the *porting organisation should allow the requesting individual to view the data (or a sample of the data which the individual has requested to be ported) before transmitting it to the receiving organisation. The requesting individual may remove data that he or she does not wish to port (e.g. unnecessary personal data of third parties).*" (emphasis added)

27. From the language used in paragraph 2.37(c), it appears that the porting organisation may elect, in its discretion, to present the requesting individual with either *all* or *a sample of* the data which the individual has requested to be ported.

28. We recognise and understand why such flexibility is required, as not all individuals would require full-detailed copies of all data before giving his or her go-ahead for the portability request to be fulfilled. That said, we propose for the individual to elect whether he or she wishes to be presented with all data or a sample of data, instead of giving this choice to the porting organisation.

29. By giving the individual the option of viewing all data held by the organisation, the individual can have full knowledge of the exact dataset being ported to the receiving organisation, and can make an informed choice as to whether to proceed with the data portability request. Depending on the volume and scale of the dataset, the porting organisation may provide the individual with a reasonable fee[17] which is commensurate with the effort required to provide the individual with such data, forming part of the individual's considerations as well. Individuals who are unable to pay the fee, assuming it is a reasonable estimate, may then elect to be presented with a sample instead.

Paragraph 2.37(d)(i) - Organisations should be allowed to charge fees to recover compliance costs of rejected/withdrawn data portability requests

30. Paragraph 2.37(d)(i) of the DPDI Consultation states that, following verification of request and individual's confirmation of the data to be ported, the porting organisation must provide the following information to the individual:

> "... *fees payable by the requesting individual, if any, for the porting. A reasonable fee may be charged to recover the cost of providing the service to port the requested data. The fees may be paid by the requesting individual or the receiving organisation. If the fees are to be borne by the receiving organisation, the porting organisation need not provide information relating to fees to the individual. The porting organisation may reject a data portability request if the individual or the receiving organisation does not agree to pay the fees. The individual may request for the PDPC to review the fees charged by the porting organisation…*" (emphasis added)

31. From a plain reading, it appears that organisations are only allowed to charge fees for recovering the cost of providing the service to port data. Therefore, if a data portability request is subsequently rejected by the porting organisation or withdrawn by the individual any time before the actual commencement of porting, it would seem that the porting organisation is unable to recover any costs whatsoever.

32. Yet, there may be costs incidental to the provision of the porting service which a porting organisation should be entitled to recover. These costs include those which relate to, but are not limited to:

    (a) ensuring the veracity of the data porting request;

    (b) informing the individual as soon as practicable of the rejection (if any) and the reason for the rejection; and

[17] See [11], *supra*.

(c) taking reasonable steps to cease (and causing its data intermediaries or agents to cease) to transmit the data, as the case may be.

33. This may be juxtaposed against Regulation 7 of the PDPR, which allows an organisation to charge an applicant who makes an access or correction request a reasonable fee for services provided to the applicant to enable the organisation to respond to the applicant's request, and regardless whether the said request is subsequently accepted by the organisation. We note that language similar to Regulation 7 of the PDPR has not been used in the present case.

34. Accordingly, we submit that an organisation should be allowed to charge a reasonable fee for services provided to the requesting individual to enable the organisation to respond to the individual's request. This is to alleviate the additional compliance costs imposed on porting organisations resulting from the Data Portability Obligation, and to ensure consistency of treatment among requests made by individuals to organisations in relation to their personal data.

Q5. What are your views on the proposed powers for PDPC to review an organisation's refusal to port data, failure to port data within a reasonable time, and fees for porting data?

35. We agree with the proposed powers referred to at paragraph 2.47 of DPDI Consultation, and note that they are consonant with the PDPC's powers in relation to an access or correction request.[18]

36. However, the proposed power referred to at paragraph 2.48 of DPDI Consultation, *viz*, the power to direct porting organisations to suspend transmission of data in certain circumstances, should be reconsidered in light of three reasons below.

37. First, whether or not personal data may be disclosed to an organisation is ultimately predicated on the consent of the individual. Barring certain exceptions that are provided for in the PDPA, the starting position for the collection, use and/or disclosure of personal data since the PDPA came into force has been that organisations are required to obtain consent from the individuals whose personal data may be affected.

38. We believe this stems from the fact that "personal data" ultimately originates from and, to a large extent, belongs to the individual who may be identified from that data. Accordingly, the individual should have the liberty to use or disclose his own personal data to any party as he pleases, provided that such use or disclosure does not directly infringe the rights of third parties (e.g. if the individual were to transmit the personal data of third parties' along with his own personal data to a receiving organisation, without obtaining the third parties' prior consent to do so).

[18] PDPA, s. 28(1).

39. Second, enforcement of the proposed power at paragraph 2.48 of the DPDI Consultation would be difficult as, under the proposed framework, the individual is already empowered to view the data to be ported or a sample thereof during the data portability request,[19] and may simply personally disclose such data to the receiving organisation himself. Notably, no equivalent power exists for the PDPC to direct suspension of disclosure *simpliciter*,[20] as here it is the *individual* who chooses to disclose such personal data.

40. Third, we note that the proposed power is not available under the existing PDPA even in relation to a transfer of personal data outside Singapore, where counterparties' risks may be higher. *A fortiori*, this power should not be available in the context of the porting of personal data to receiving organisations "*that have a presence in Singapore*".[21]

41. Although the concern about preventing information of a sensitive nature (e.g. bank account details) from falling into the wrong hands is understandable, this concern may be addressed by the "*consumer safeguards*" and "*counterparty assurance*" to be set out in the relevant codes of practice for specific sectors.[22]

Q7. What are your views on the proposed approach for organisations to use personal data for the specified businesses innovation purposes, without the requirement to notify and seek consent to use the personal data for these purpose?

42. Paragraph 3.5 of the DPDI Consultation states that:

> "*... organisations may use personal data for business innovation purposes without the requirement to notify the individuals of and seek consent to use their data for these purposes. However, for the collection or disclosure of personal data, whether for business innovation purposes or other purposes, organisations must notify and seek consent, unless there is an applicable exception to consent in the Second or Fourth Schedule to the PDPA.*" (emphasis added)

43. Further, paragraph 3.10 of the DPDI Consultation states that "*business innovation purposes specified in paragraph 3.3 will be considered business purposes for which retention of the personal data may be necessary.*" (emphasis added)

[19] DPDI Consultation, at para 2.37(c).

[20] While PDPA, ss. 29(1)-(2) empower the PDPC to "*give the organisation such directions as the Commission thinks fit to ensure compliance with [any provision in Parts III to VI]*" and to "*give the organisation all or any of the following directions: (a) to stop collecting, using or disclosing personal data in contravention of this Act. [...]*", we emphasise that such powers to direct are only available to the PDPC for instances of non-compliance or contraventions of the Act, and further only as against *organisations* and not the *individuals.*

[21] DPDI Consultation, at para 2.18.

[22] DPDI Consultation, at para 2.49(a)-(b).

44. Considering the potentially wide scope of "business innovation purposes",[23] and reading paragraphs 3.5 and 3.10 together, we are of the view that organisations could potentially rely on business innovation purposes to use and retain personal data previously collected for indefinite periods of time,[24] notwithstanding individuals' withdrawal of consent to organisations' use and disclosure of their personal data for all purposes. Therefore, we urge the PDPC to consider reinstating the requirement to notify and seek consent to use personal data for business innovation purposes. While many companies may already include purposes similar or akin to business innovation in their privacy notices, it is nevertheless vital that consent be obtained from these individuals to use their personal data for business innovation purposes, especially in light of the consent-centric framework that the PDPC has established for the collection, use and/or disclosure of personal data by organisations.[25]

45. Alternatively, if the PDPC maintains that consent should not be required to use personal data for business innovation purposes, we suggest imposing a time limit (e.g. one year) calculated from the date an individual notifies[26] the organisation to stop using his or her personal data for business innovation purposes. In such a scenario, while consent is not required for organisations to use personal data for business innovation purposes, the individual remains in control of his personal data by being able to stop such use for any reason whatsoever. Nonetheless, the efficacy of this safeguard is predicated on the time limit being reasonable and not unduly lengthy, so as to give effect to the individual's wishes.

46. While we appreciate the utility in allowing organisations to use personal data to develop better services and products, we believe an appropriate balance should be struck with an individual's freedom to decide whether and how his or her personal data is used.

Conclusion

47. We appreciate the PDPC's efforts to protect the interests of individuals while ensuring that business innovation and operations are not unduly stifled. We are grateful for the opportunity to submit our views, and would be happy to address any queries that the PDPC may have in relation to our submissions.

[23] DPDI Consultation, at para 3.3, referring to the purposes of (i) operational efficiency and service improvements; (ii) product and service development; or (iii) knowing customers better.
[24] DPDI Consultation, at para 3.9 - 3.10. An organisation is allowed to retain personal data, even after the individual withdraws consent, so long as it is necessary for a legal or business purpose (the latter of which includes a business innovation purpose).
[25] Lim Jeffrey, Sui Yin and Lee Yue Lin, "Data Sharing: When Consent is Not Enough" [2018] PDP Digest 90 at [4].
[26] We note that an individual cannot "withdraw consent" for a purpose to which consent was never first given.