WONGPARTNERSHIP LLP

RESPONSE TO THE PERSONAL DATA PROTECTION COMMISSION'S CONSULTATION PAPER ON REVIEW OF THE PERSONAL DATA PROTECTION ACT 2012 –

PROPOSED DATA PORTABILITY AND DATA INNOVATION PROVISIONS

WONGPARTNERSHIP LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982

1. INTRODUCTION

1.1 We wish to thank the Personal Data Protection Commission ("**PDPC**") for the opportunity to comment on the *Public Consultation on Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions* (issued 22 May 2019) ("**Public Consultation**").[1]

1.2 As one of Singapore's largest and leading law firms, with many clients in the public infrastructure space, financial services, telecommunications, essential services, as well as technology sectors, we are keen to share our thoughts and concerns in relation to the Public Consultation, as it may have material impacts on many of our clients in relation to their collection, use, disclosure, and processing of personal data under the Personal Data Protection Act (No. 26 of 2012 of Singapore) ("**PDPA**") in Singapore.

1.3 In preparing our responses herein, we have had discussions with our clients to understand their concerns. We are fully supportive of the PDPC's efforts to engage in stakeholder discussions, and would be happy to further discuss or elaborate on any of the points submitted upon.

1.4 Following our review of the proposed data portability and data innovation provisions, as well as the questions posed in the Public Consultation, we are pleased to provide our comments below and highlight some concerns which we think merit further deliberation and consideration.

2. QUESTION 1

What are your views on the impact of data portability, specifically on consumers, market and economy?

2.1 In paragraph 2.14 of the Public Consultation, the PDPC proposes that an organisation must, at the request of the individual, provide the individual's data that is in the organisation's possession or under its control, to be transmitted to another organisation in a commonly used machine-readable format ("**Data Portability Obligation**").

2.2 We agree that the proposed Data Portability Obligation has potential to promote consumer welfare by providing consumers with greater choice and control over their data held by the organisations, and enable greater data flows between organisations (and thereby have a positive impact on the growth of Singapore's digital economy).

2.3 As noted in the Discussion Paper on Data Portability published by the PDPC in collaboration with the Competition and Consumer Commission of Singapore (issued 25 February 2019) ("**Discussion Paper**"),[2] the proposed Data Portability Obligation may also have the effect of encouraging greater market competition in Singapore's emerging digital economy by minimising "switching costs" between organisations, thereby lowering the barriers to entry and expansion for the market players: *ibid*, at paragraph 3.17.

2.4 However, while the proposed Data Portability Obligation has potential to generate some pro-competitive effects in the market, such benefits should also be weighed against the potential for significant market distortions.

2.5 In particular, as the PDPC recognised in paragraph 3.18 of the Discussion Paper, consumers may naturally gravitate to join the dominant network so as to take the benefit of pre-existing network effects, and the proposed Data Portability Obligation may serve to entrench existing

[1] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/PDPC-Public-Consultation-Paper-on-Data-Portability-and-Data-Innovation-Provisions-(220519).pdf
[2] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf

dominant networks, precisely by making it easy for users to switch to the dominant network, leading to increased market concentration.

2.6 On the one hand, the introduction of the data portability requirement means that consumers may enjoy greater ease of switching from one service provider to another service provider, thus theoretically benefiting smaller players in the market in reducing barriers to consumer data.

2.7 On the other hand, under the Proposed Data Portability Obligation, the individual has the ultimate discretion as to the exercise of the right to data portability, the organisation it wishes to transmit the data to, as well as the data which ought to be transmitted. Consequently, any perceived competitive pressure from the smaller service providers arising from the introduction of the data portability requirement remains theoretical until the actual exercise of the right by the requesting individual to port data.

2.8 Ultimately, especially in markets characterised by strong network externalities, the value of the network increases as more users join the network, and it should not be assumed that consumers would always exercise their right to port data to smaller service providers from larger service providers. Indeed, we think that it is reasonably conceivable that users may exercise their right to port data from smaller service providers to switch to dominant service providers to take advantage of pre-existing network externalities already enjoyed by dominant service providers.

3. **QUESTION 2**

What are your views on the proposed Data Portability Obligation, specifically – (i) scope of organisation covered; and (ii) scope of data covered?

3.1 As to the scope of the proposed Data Portability Obligation, we are especially concerned about the scope of data proposed to be covered. If the scope of data covered is too expansive (e.g. going beyond personal data), potential market entrants may be deterred by the fear that expansive amounts of data within the scope of the proposed Data Portability Obligation (and in the organisation's possession or under its control) could be required by law to be transmitted to another organisation (including its market competitors) from time to time.

3.2 Hence, the scope of data covered by the Data Portability Obligation merits closer consideration. After all, the introduction of such an expansive data portability requirement could affect Singapore's reputation as an attractive location as a regional base for businesses, especially from the perspective of data-intensive international companies.

3.3 In this regard, we propose to limit the scope of data covered by the Data Portability Obligation to personal data of the requesting individual (not extending to third parties).

(a) Limit to Personal Data

In paragraph 2.24 of the Public Consultation, PDPC proposes that, subject to certain exceptions, the proposed Data Portability Obligation extend beyond personal data, to include any data that is: (i) provided by the individual to the organisation ("**user provided data**"); and (ii) generated by the individual's activities in using the organisation's product or service ("**user activity data**"), to the extent that such data is in the possession or control of the organisation and is held in electronic form.

User provided data and user activity data are conceptually broader than personal data (as defined under the PDPA), and may include the individual's business contact information, as well as personal data of third parties (insofar as provided by the requesting individual or generated by the individual's activities): paragraphs 2.29 and 2.30 of the Public Consultation.

However, by extending the scope of the data covered beyond personal data, this could generate inconsistencies within the existing data protection framework and existing global norms, and may also generate onerous compliance costs for the organisations as follows:

(i) Consistency in the PDPA Framework

In principle, the proposed Data Portability Obligation should be limited to the requesting individual's personal data, insofar as the Access Obligation is only limited to the requesting individual's personal data. After all, the proposed Data Portability Obligation is intended to be complementary extension of section 21 of the PDPA ("**Access Obligation**"): see paragraph 2.43 of the Public Consultation; i.e. by extending the ability of individuals to access their personal data (held by an organisation) to the ability to transmit their personal data (to another organisation).

Furthermore, the existing data protection framework under the PDPA is intended to govern the collection, use and disclosure of personal data by organisations in Singapore. If the scope of the proposed Data Portability Obligation applies to data beyond the existing definition of personal data under the PDPA, it would also be unclear as to how such an obligation would interact with the existing statutory framework (e.g. personal data collected without consent under the Second Schedule of the PDPA, or personal data of third parties).

(ii) Consistency with International Trends

We also note that many jurisdictions have limited the scope of the data covered to the individual's personal data. Such a limitation would therefore be consistent with international trends of not overextending the ambit of personal data protection frameworks to regulate more than "personal data".

"Personal data" is a well-established concept that is recognised internationally in various national-level data protection frameworks,[3] and we have made comparisons with other jurisdictions which have introduced data portability requirements. For example, we note that the data subject's right to data portability under Article 20 of the General Data Protection Regulation ("**GDPR**") of the European Union is limited to personal data concerning the data subject which he or she has provided to the organisation. As the Article 29 Data Protection Working Party confirmed in the Guidelines on the right to data portability (as last revised and adopted on 5 April 2019) ("**WP29 Guidelines**"), only "personal" data falls within the scope of the Article 20 data portability request, and any data that has been anonymised or does not concern the individual will not be subject to the data portability request under the GDPR.

In our view, limiting the proposed Data Portability Obligation to apply only to personal data would, in principle, strike a better balance between legitimate organisational interests in data flows and the need for protecting individuals' personal data.

(iii) Minimising Compliance Costs

[3] For example, please see OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data which defines "personal data" as "any information relating to an identified or identifiable individual (data subject)".

Additionally, we submit that limiting the proposed Data Portability Obligation to personal data of the requesting individual would tend to minimise compliance costs.

We note that there has been some discussion concerning proper calibration of compliance costs imposed by the proposed Data Portability Obligation (as well as the correct balance to strike) – see, e.g. paragraphs 4.18 to 4.12, and paragraph 5.2 of the Discussion Paper; see also paragraphs 2.8 to 2.10 of the Public Consultation (where the PDPC recognised, inter alia, that having a "*Data Portability Obligation which covers an overly broad spectrum of data would … impose compliance costs [and] could also have a dampening effect on innovation*").

In particular, we note from paragraph 2.8 of the Public Consultation that the PDPC is of the view that compliance costs for GDPR-compliant organisations under the proposed Data Portability Obligation would likely be limited to the "*incremental cost of extending the data portability service to Singapore*".

However, in this regard, we think that compliance costs would only truly be "incremental" if the scope of the proposed Data Portability Obligation becomes limited to personal data, especially because the data portability obligation under the EU framework is in fact limited to personal data only: see our discussion above concerning the Article 20 data portability request under the GDPR regime.

Indeed, systems which are currently built for compliance with the PDPA (and/or other relevant data protection laws in other jurisdictions) should already manage data access and correction requests from individuals concerning their personal data. Where the scope of the data covered under the proposed Data Portability Obligation is wider than personal data, there may be a need for organisations to carry out extensive data audits and reconfigure their systems (currently calibrated to manage only personal data), thereby incurring significant and potentially non-incremental compliance costs.

(b) Limit to Personal Data the Requesting Individual (not extending to Third Parties)

We propose that the scope of data covered under the proposed Data Portability Obligation should not extend to include the "personal data of third parties".

In paragraphs 2.30 to 2.31 of the Public Consultation, the PDPC proposes that the scope of the proposed Data Portability Obligation should also include personal data of third parties, so long as it was provided by the requesting individual, or generated by the individual's activities.

In this regard, PDPC stated 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. In particular, under the proposed framework, 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.

Despite the above-mentioned safeguards, we are of the view that the Data Portability Obligation should not extend to personal data of third parties for the following reasons:

(i) Difficulty in Enforcing Safeguards

First, unless the PDPC investigates in a specific case, in many cases the porting and receiving organisations, as well as the requesting individual, would be the parties deciding if the comingled personal data of third parties (in user activity data) are appropriately included as part of the data requested to be ported without regulatory scrutiny – and significantly, the third party to whom the data relates is *not* part of this decision-making process.

In addition, while the porting organisation has little incentive to reduce the amount of data ported (save perhaps for confidential or proprietary data), the receiving organisation is likely to have incentive to receive as much data as possible. Moral hazard could arise under such an arrangement because the requesting individual also has little incentive to limit exposure of third parties data (insofar as they do not concern the individual).

It would therefore be difficult third parties to monitor whether their personal data (as comingled with data of other individuals) have in each case been appropriately ported and used only for the requesting individual's own personal or domestic purposes. Indeed, the relevant third party would not even be notified.

Hence, if the Data Portability Obligation extends to personal data of third parties, it remains unclear whether there are adequate safeguards in determining whether such personal data of third parties would be properly included or used by the receiving organisation.

(ii) Inconsistent with Consent-Based Regime

Second, from the perspective of a consent-based regime for personal data protection, we are also concerned that there appears to little basis, in principle, for the dispensation of the requirement of third parties' consent in respect of the sharing of these third parties' personal data even if such "*data is under the control of the requesting individual and used only for that individual's own personal or domestic purpose*".

There is also no clear legal basis under the existing PDPA for the disclosure of third parties' personal data by the porting organisation, nor are there any clear legal basis for the collection and usage of these third parties' personal data without consent: see also our discussion above concerning the lack clarity as to the interaction of the proposed Data Portability Obligation with existing statutory exceptions.

Comparing also with international trends (for example, the WP29 Guidelines clarified that where personal data of third parties is included in the data set to be ported pursuant to Article 20 of the GDPR), we are of the view that there is a need to identify the proper legal basis for the processing, such as obtaining the necessary consent from the individual or where there the data processing is necessary for the purposes of some legitimate interests pursued by the organisation.

(iii) Consistency with Access Obligation.

Third, on the basis that the proposed Data Portability Obligation is intended to be complementary to the Access Obligation, it may be difficult to justify why the existing exceptions in relation to third parties' personal data (i.e. where compliance with the access request would reveal personal data about another individual or reveal the identity of an individual who has provided personal data

about another individual and the individual providing the personal data does not consent to the disclosure of his identity) should not apply mutatis mutandis to the Data Portability Obligation: see paragraph 2.45 of the Public Consultation, where the PDPC proposes to align the exceptions to the proposed Data Portability Obligation with the exceptions to Access Obligation, except for the prohibitions provided for situations where it involves third party data in user activity data.

4. **QUESTION 3**

What are your views on the proposed exceptions to the Data Portability Obligation, specifically – (i) the proposed exception relating to the commercial confidential information that could harm the competitive position of the organisation, to strike a balance between consumer interests and preserving the incentive for first movers' business innovation; and (ii) the proposed exception for "derived data"?

4.1 We agree that, in principle, the proposed exceptions to the Data Portability Obligation ought to be aligned to the exceptions to the Access obligation on the basis that the Data Portability Obligation is intended to be complementary to the Access Obligation.

4.2 In this regard, we would highlight some concerns about the proposed exception for "*data which, if disclosed, would reveal confidential commercial information that could harm the competitive position of the organisation*" ("**Confidentiality Exception**") and the proposed exception for derived data ("**Derived Data Exception**").

(a) Confidentiality Exception

We agree that proposed Data Portability Obligation should, in principle, be subject to the exception relating to commercial confidential information that could harm the competitive position of the organisation to preserve the rights of the organisations and also the incentive for first movers' business innovation.

As recognised in paragraph 2.10 of the Public Consultation, there is a need to consider the interests of the "first movers" in innovation, "fast followers" and "new entrants", and we note that the PDPC has indeed proposed the Confidentiality Exception in order to protect first movers who bring to market an innovative product or service from unfair competition by fast followers.

Nevertheless, as a preliminary point, we find that the scope of the proposed Confidentiality Exception and the kind of data which would suffice to constitute "*confidential commercial information that could harm … competitive position*" seems unclear. For example, would "user activity data" gathered as part of the organisation's trial of their products and services fall within the scope of the proposed Confidentiality Exception? In the biomedical industries, these trial data would likely constitute valuable proprietary information for the development and refinement of their products and services, and the subsequent application for the necessary product approval with the relevant regulators.

More significantly, it may be helpful for PDPC to clarify how the Confidentiality Exception may also extend to protect intellectual property rights (or trade secrets), as well as proprietary data processing methodologies. These concerns are discussed in more detail as follows:

(i) Protection of Intellectual Property Rights and Trade Secrets

First, while the proposed Confidentiality Exception preserves some of the organisation's rights insofar as these data constitute confidential commercial information, greater clarity may be required as to the interaction between the proposed Data Portability Obligation and the protection of intellectual property rights and trade secrets of the organisation under the law.

For example, it may be helpful if the PDPC could expressly stipulate that the Data Portability Obligation shall in any event be subject to the organisation's rights under other law (e.g. intellectual property rights).

By way of comparison, Article 20(4) of the GDPR provides that the data subject's right to data portability "shall not adversely affect the rights and freedoms of others", which may include trade secrets or intellectual property and in particular the copyright protecting the software.[4]

Ultimately the proposed Data Portability obligation should not be allowed to allow individuals to misuse the information in a way that would constitute a violation of intellectual property rights.

(ii) Protection of Confidential and Proprietary Data Processing Methodologies

Second, following from our analysis above regarding extending the scope of the proposed Data Portability Obligation as extending to beyond "personal data", we further submit that there may be a dampening effect on innovation if data falling within the proposed Data Portability Obligation is not limited to personal data, because the proposed Confidentiality Exception (as currently worded) may not be sufficient to address the potential erosion of commercial incentives for constant innovation in the market.

Specifically, the proposed Confidentiality Exception only addresses cases where the competitive edge of the organisation is derived from the data itself (i.e. where the *substance* of the data is confidential), but does not seem to protect organisations in cases where it is the *methodology* of processing data that is proprietary and sensitive.

However, in data-heavy industries, including many financial services, e-commerce and entertainment businesses, an organisation's competitive advantage may lie precisely in that organisation’s capabilities in data collection processes (e.g. their ability to collect and parse data to tailor their products and services for their users).

In this regard, notwithstanding the proposed Confidentiality Exception, the introduction of the data portability requirement beyond the scope of personal data may erode precisely that edge of being able to process "user activity data" in large volumes and in particular ways.

For example, the value of an organisation in the artificial intelligence ("**AI**") industry would be largely driven by the amount of data the organisation is able to collect, including the availability of user-activity data used to train their AI algorithms. Similarly, significant investments are made by organisations to build up the organisations’ capabilities to collect and process large amounts of data as well as the collection and proprietary methodologies to curate (or “clean”) these data sets, sometimes known as “cleaning” models) to meaningfully understand raw user activity data. However, if organisations are

[4] Article 29 Data Protection Working Party confirmed in the Guidelines on the right to data portability (as last revised and adopted on 5 April 2019) at page 12.

obliged to port user activity data post-treatment by such proprietary methodologies, the competitive edge of businesses who generate value from treating data could be eroded, creating a dampening effect on innovation.

(b) Derived Data Exception

The PDPC proposes that, under the Derived Data Exception, "derived data" (which refers to new data that is created through the processing of other data by applying business-specific logic or rules) should be excluded from the scope of the Data Portability Obligation: see paragraph 2.28 of the Public Consultation.

Since “processing” for the purposes of the definition of “derived data” is intended to be defined broadly to include the use of any mathematical, logical, statistical, computational, algorithmic, or analytical methods (see footnote 13 of the Public Consultation), we recommend that there be greater clarity on what is to be regarded to as "business-specific logic or rules", such as introducing a *de minimis* threshold for the concept of "derived data".

Otherwise, the potential scope of data created through the processing of data using business-specific rules may be unclear.

In this regard, we note that the illustrations provided in the Public Consultation suggest that “derived data” is generally intended to refer to insights generated from data analysis (or processed data of similar nature). However, a plain reading of the proposed “derived data” exception raises the question whether any raw data (i.e. user provided data or user activity data) that is processed by the organisation, howsoever minimally, would become "derived data" so as to be excluded from the Data Portability Obligation.

Would user activity data which is automatically aggregated, processed and compiled (even if token or minimal) for the organisation's analysis constitute derived data, thereby falling outside the scope of the proposed Data Portability Obligation? For example, the processing of NRIC numbers to partial NRIC number or the processing of national identification numbers to create alternative identifiers would appear to fall under the definition of derived data, and therefore excluded from the Data Portability Obligation. Similarly, would the mere creation of a simple index result in the dataset becoming “derived data”, and therefore fall outside of porting requirements?

5. **QUESTION 4**

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

5.1 We note that the transmission of the data by the porting organisation may ultimately be subject to acceptance of the ported data by the receiving organisation (at least if the receiving organisation deems that the data is “irrelevant” or “excessive”): see paragraphs 2.37(d)(ii) and 2.39 of the Public Consultation.

5.2 In this regard, we are of the view that the PDPC should prescribe with greater clarity the legal test for determining *when* the porting organisation would deemed to have discharged its obligation port data to the receiving organisation, especially in relation to the required: (a) data formats and structures; and (b) porting timelines.

(a) Data Formats and Structures

We note that the PDPC has proposed that it will not prescribe the data formats that an organisation should adopt for transmitting data, though it recommends that “*formats used should be easily accessible and affordable to any organisation receiving the data*”,

"*transmit and receive data in a common, machine-readable format*" and "*where possible, open data formats should be used*": see paragraph 2.37(e) of the Public Consultation.

However, without a clear stipulation as to the data format acceptable for porting, we are concerned that there may be uncertainty surrounding whether the porting organisation or the receiving organisation has sufficiently performed its obligations where issues arise in relation to the interoperability of the ported data set (including issues with the format and/or data structures), as well as the receiving organisation's computer systems and databases.

In this regard, we propose that PDPC should expressly prescribe that data ported pursuant to the Data Portability Obligation **must** be in open data formats, easily accessible, reasonably affordable to any organisation receiving the data, and not subject to costly licensing agreements as alluded to by the PDPC in paragraph 2.37(e) of the Public Consultation.

While we note that there are perhaps "*no internationally defined or developed standards to address data portability*" presently (see paragraph 4.4 of the Discussion Paper), expressly prescribing the requirement of data transmission via affordable, open formats would: (i) provide clear legal criteria for PDPC to review in cases where, e.g. there are allegations of defective transmission; and (ii) tend to lower compliance costs because porting organisations would have greater certainty in discharging their obligations where an open format is used for transmission, and also correspondingly reduce the complexity of data interoperability on the part of receiving organisations.

We also are of the view that prescribing a common interface for both transferor and transferee organisations to meet will not be meaningful, given that each organisation will have its own data structures. We therefore think that a more practical solution will be for transferor organisations to discharge their obligations by providing information in an open standard data format, and for the transferee organisation to address the ingestion of such data into its own databases.

Transferor organisations should also have the right to restructure or reorganise their exported data as they would legitimately have concerns about protecting their intellectual property rights in the database schemas, or the exported data disclosing how their systems are designed, which can also give rise to security risks.

(b) Porting Timelines

We note that the PDPC proposes to prescribe in the regulations that, subject to specific codes of practice, the porting organisation would only have seven calendar days to comply with the porting request following the verification of the porting request and upon the individual's confirmation of the data to be ported.

However, depending on the complexity of the formats and structures required for the transmission of data, complete porting could reasonably require more than seven calendar days.

For consistency, we propose for the timeframe to be aligned with the Access Obligation (i.e. the organisation must port the data as soon as reasonably practicable from the time it receives the individual's request to port data. If the organisation is unable to comply with the requirement within 30 calendar days from the time it receives the request, it must inform the individual of when it will respond to the request within that time).

5.3 In addition, to further manage compliance costs, we agree with the PDPC that the porting organisation should be allowed to charge reasonable fees to recover the cost of providing the service to port the requested data: see paragraph 2.37(d)(i) of the Public Consultation, and that the porting organisation may reject a data portability request if the requesting individual does not agree to pay the fees. The transferee organisation can similarly charge fees to ingest the data into its databases, though of course the transferee organisation may still decide not to do so for its own commercial reasons.

5.4 This would also be consistent with the existing statutory position taken in relation to access requests under the PDPA, where the consumer should bear reasonable fees for the transmission of data as the porting is ultimately for his/her benefit.

6. **QUESTION 5**

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?

6.1 At the outset, perhaps the PDPC should adopt a light touch approach to give the market time to adapt and also to establish market norms. In any event, the review of issues such as failure to port data within a reasonable time, and fees for porting data will be more technically complex and perhaps redress should only be phased in at a later time.

7. **QUESTION 6**

What are your views on the proposed binding codes of practices that set out specific requirements and standards for the porting of data in specific clusters or sectors?

7.1 We agree that there should be sectoral codes of practices to address specific issues surrounding data portability which may be ultimately sector-specific. For example, the medical services sector may wish to implement a harmonised machine-readable format to promote interoperability amongst the healthcare electronic systems. Similarly, in the financial services industry, there may also be concerns surrounding the compliance of Monetary Authority of Singapore's outsourcing rules as well as technology risk management guidelines.

7.2 These should also be tempered against security related concerns, eg. the portability rules should not apply in relation to systems which are critical information infrastructures designated under the Cybersecurity Act, or other sensitive systems, and transferor obligations should have the ability to reject requests for data ports on account of such concerns.

8. **QUESTION 7**

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

We agree that the proposed approach for organisations to use personal data for the specified business innovation purposes without the requirement to notify and seek consent to use the personal data for these purpose ("**Business Innovation Exception**") would go towards enabling organisations to use data with more regulatory certainty in order to derive business insights and innovate in the development and delivery of products and services.

However, the PDPC should in this context also clarify the law on the following two issues:

(a) Aggregated Insights

First, we would like to clarify, whether, under the proposed Business Innovation Exception, if multiple organisations engage in a single data processor to use such data for their respectively specified business innovation purposes, whether such a data processor would in turn be allowed to use all received personal data (from multiple organisations) to benefit the respective organisations up-stream.

For example, would a third party service provider be allowed to aggregate all the personal data it has collected from multiple organisations to derive business insights to help the respective organisations further refine and develop their respective products and services?

(b) Alignment with Telecommunications Act and Telecom Codes Frameworks

Second, the proposed Business Innovation Exception should be harmonised with other existing frameworks (insofar of course, that any derived data or data insights will not be identifiable to particular individuals), eg. telecommunications service providers who derive insights from personal data of its customers for business innovation purposes without notification or consent would not breach Section 42 of the Telecommunications Act (Cap 323, Rev 2000) ("**TA**"). Likewise, this should also not trigger Banking Act concerns in respect of banking secrecy.

In the same vein, PDPC should also expressly clarify the interaction between the proposed Business Innovation Exception, Section 42 of the TA, and the provisions in the *Code of Practice for Competition in the Provision of Telecommunication Services 2012* ("**Telecom Code 2012**") concerning End User Service Information ("**EUSI**").

EUSI potentially comprise personal data of end users of telecommunication services, including, e.g. an end user's location information, billing address, name, address, credit history, usage patterns, etc: see paragraph 3.2.6.1 of the Telecom Code 2012.

Under the Telecom Code 2012, a telecommunication licensee may provide EUSI of its business end users to third parties (including affiliates) for the purposes of, inter alia, developing goods and services provided that consent of such end users have been obtained: see *ibid* at paragraph 3.2.6.2(b). Similarly, for residential end users, a telecommunication licensee may only collect, use, and/or EUSI "in accordance with, or as permitted under, any applicable laws" relating to the use of personal data, including under the PDPA: see paragraph 3.2.6.2(d) of the Telecom Code 2012.

For consistency, if notification or consent is not required under the proposed Business Innovation Exception, similarly, the derivation of insights using EUSI data should no longer require consent.

9. **QUESTION 8**

What are your views on the proposed definition of "derived data"?

Please see our comments above under Question 3.

10. **QUESTION 9**

What are your views on the proposal for the Access, Correction and proposed Data Portability Obligations not to apply to derived personal data?

Please see our comments above under Question 3.

11. CONCLUSION

11.1 In conclusion, we agree that, in light of the emerging digital economy, there is a need to provide a balanced regulatory approach to support innovation in a digital economy whilst giving consumers meaningful choice and control over their personal data. The driving vision for the proposed data portability and data innovation provisions should be to enable Singapore's data protection framework to be in step with global regulatory trends and practices, as well as cater to the needs of businesses and individuals in the evolving digital economy.

11.2 The imposition of data portability requirements as proposed will likely also translate into significant business costs, and also raise other concerns in relation to the protection of intellectual property, confidentiality and cybersecurity. Hence, PDPC may wish to provide greater clarity and guidance in connection with the proposed data portability and data innovation provisions as discussed above, and also allow organisations more flexibility and leeway in the manner in which the obligations may be addressed.

11.3 In light of the foregoing, we respectfully request that the PDPC consider these issues when introducing the relevant amendments to the PDPA framework for the collection, use and disclosure of personal data in Singapore.

WONGPARTNERSHIP LLP

17 July 2019