PUBLIC CONSULTATION ON REVIEW OF THE PERSONAL DATA PROTECTION ACT 2012 – PROPOSED DATA PORTABILITY AND DATA INNOVATION PROVISIONS

ISSUED 22 MAY 2019

TABLE OF CONTENTS

PART I: INTRODUCTION AND BACKGROUND

1.1 This consultation seeks feedback and input from relevant stakeholders and interested parties on the proposal to introduce provisions for data portability and data innovation under Singapore's Personal Data Protection Act 2012 ("PDPA"). This proposal is part of the review of the PDPA by the Personal Data Protection Commission ("PDPC").

1.2 The PDPA was enacted in 2012 to govern the collection, use and disclosure of personal data in Singapore. It seeks to strike a balance between the need to protect individuals' personal data against organisations' need to collect, use and disclose personal data for legitimate and reasonable purposes. Its two key sets of provisions, the Do Not Call Provisions and the Data Protection Provisions, came into effect on 2 January 2014 and 2 July 2014 respectively.

1.3 One of the key aims of the ongoing PDPA review is to strengthen accountability among organisations and consumer trust in the management of personal data. In line with these objectives, PDPC is considering the introduction of data portability and data innovation provisions under the PDPA.

1.4 Data portability gives individuals greater control over their personal data by allowing them to request for their data held by an organisation to be transmitted to another organisation in a commonly used machine-readable format. This will enable individuals to move their data across services and enable greater access to more data by organisations. The proposed data innovation provisions complement this by making clear that organisations can use data for appropriate business purposes. Collectively, PDPC believes these will help spur the development of new and innovative products and services that will benefit consumers and support the growth of the Digital Economy.

PART II: PROPOSED DATA PORTABILITY OBLIGATION

A. Impact of Data Portability

2.1 In assessing the introduction of a Data Portability Obligation in Singapore, the following impacts were considered.

Consumer impact

2.2 As a consumer right, data portability provides consumers more choice and control over their data held by organisations. When consumers are able to move their data easily from one service provider to another, consumers are better empowered to try out or move to new or competing service offerings that may better suit their needs. Organisations may also be incentivised, with access to historical data of prospective customers, to provide more competitive offers.

2.3 Data portability allows consumers to move from one service provider to another without losing past records and important histories built up with the previous service provider. For example, an individual's loan or credit repayments and purchase histories, built up over the years with a bank, can potentially be moved to another bank to benefit from more attractive services offered. This overcomes consumer lock-in with one service provider, and is particularly useful when existing providers are going out of business. Data portability can also help ease the burden of backing up and refurnishing personal data when switching to other service providers. Consumers can also benefit from faster service delivery, such as shorter processing duration for insurance or loan applications as data portability potentially reduces the time taken to obtain customers' data.

2.4	**Example** Sally has an existing account with online shopping platform ABC. She would now like to switch to online shopping platform XYZ to enjoy better membership services and benefits offered by XYZ. With data portability, Sally will be able to request for ABC to transmit her personal data, indicated preferences, past shopping history and transactions etc, to XYZ so that she can enjoy the benefits offered by XYZ taking into account her past transactions, while retaining important records of past orders and purchases with ABC.

Market impact

2.5 Data portability is envisaged to have a positive impact on the growth of the Digital Economy by enabling greater data flows which support data innovation.

2.4 Much of the data collected, generated and held by organisations today is being analysed in silos, in part due to a lack of standards and interoperability of systems. This limits greater use of data and potential benefits that can be reaped from cross-sectoral use of data. New entrants may also face barriers to entry where they are unable to collect or access the same kind of data that established companies have access to.

2.5 Data portability provides a way to overcome such data silos and barriers. With data portability, friction is reduced for data to be acquired. Organisations will have greater access to consumers' data held in silos, and this helps reduce barriers to entry, particularly for start-ups or small players in sectors that are heavily reliant on consumer data. Data portability could be a key enabler of inter-organisation and even cross-sector data flows. With access to more data, organisations can use the data to glean new insights to better understand their customers and improve their products and services to better meet their customers' needs. Data can be used and combined in new ways, thereby enabling the growth of new business models and services in the Digital Economy.

2.6 Examples from countries that have introduced data portability support this proposition. The UK's Open Banking initiative has enabled the creation of a new app that allows consumers to consolidate their accounts from multiple banks[1]. The industry also recognises the value in data portability. For instance, the Data Transfer Project ("DTP") is an industry-led initiative to provide users with the ability to move their data between different online platforms[2]. Potential use cases for individuals include trying out another service, leaving a service, and backing up their data.

2.7	**Example** John is a customer of Telecommunications Service Provider A and would like to provide Travel Services Provider B data about his overseas mobile phone usage in order to benefit from B's customised travel planning services. He can request to port his overseas mobile phone usage data from Telecommunications Service Provider A to Travel Services Provider B. Travel Service Provider B will be able to use the data to derive insights on John's past travel locations and patterns based on his mobile phone usage trends to develop customised travel services and recommendations to meet John's needs. In addition, Travel Service Provider B may also be able to draw on aggregated data of customers' profile to come up with new travel products and services for its customers.

[1] "UK moving from 'open banking' to 'open finance'", January 2019, https://www.out-law.com/en/articles/2019/january/uk-moving-from-open-banking-to-open-finance
[2] https://datatransferproject.dev

2.8 PDPC is mindful that introducing a Data Portability Obligation may result in additional compliance costs for organisations. PDPC notes that organisations which operate in the EU are already required to comply with a data portability right under the EU General Data Protection Regulation ("GDPR"). For such organisations, compliance cost may be limited to the incremental cost of extending the data portability service to Singapore. The introduction of data portability in Singapore will create the impetus for companies that have developed data portability functionalities to extend these to consumers in Singapore.

2.9 Data portability could also have the effect of raising the barriers to entry, if new service providers view the requirements too burdensome[3]. For a small company with voluminous historical records, initial compliance costs could be significant if they hold large amounts of customer data and these compliance costs may represent a barrier expansion.

2.10 PDPC recognises the need to consider the interests of the individuals as well as organisations - such as the first movers in innovation, fast followers, and new entrants. PDPC is mindful that a Data Portability Obligation which covers an overly broad spectrum of data would not only impose compliance costs, it could also have a dampening effect on innovation. Organisations must innovate in order to entice customers to use their products or services. However, first movers may not be incentivised to innovate if a fast follower can emulate its business model and easily acquire its customers' data through the Data Portability Obligation. It is therefore important to create the right competitive landscape in order to strike a balance and reap the most benefits for consumers and the economy.

International developments

2.11 Internationally, the right to data portability has been introduced in the European Union ("EU"), Australia and the Philippines. Several other jurisdictions such as India, Japan, New Zealand and United States (States of California) are also considering the introduction of the right to data portability in their domestic laws.

2.12 In general, the right to data portability bears the following features. First, the individual has the right to receive the personal data concerning him or her, which he or she has provided to the organisation.[4] Second, the personal data is to be ported in a structured, commonly used and machine-readable format. Third, the personal data is to be transmitted directly from one organisation to another[5].

[3] Aysem Dike Vanberg, 'The Right to Data Portability in the GDPR: What Lessons Can Be Learned From the EU Experience' (2018) 21(7) *Journal of Internet Law.*

[4] In the European Data Protection Board's ("EDPB") Guidelines on the right to data portability, the EDPB considers 'provided to a controller' to cover data provided knowingly and actively by the data subject, as well as the personal data observed from his or her activity. Under Australia's Consumer Data Right, consumers are granted open access to their banking, energy, telephone and internet transactions.

[5] See Article 20 and Recital 68 of the GDPR. Under US California's Consumer Privacy Act, requested information is provided to the consumer to provide to another organisation.

2.13 In reviewing the PDPA, it is imperative to ensure that it keeps pace with international data protection developments and aligned with the data protection regimes of key jurisdictions. Alignment with international data protection standards will enable Singapore's regime to be recognised by these jurisdictions, supporting Singapore's larger objective in facilitating cross border data flows. As one of the pioneering countries to consider the introduction of data portability will also allow Singapore to remain ahead of the curve and for the PDPA to be viewed as progressive internationally.

B. Proposed Data Portability Obligation

2.14 PDPC is considering the introduction of a Data Portability Obligation under the PDPA. Under the proposed obligation, 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**.

2.15 The following sections describe in further detail the proposed obligation and the conditions under which the proposed obligation applies.

Covered organisations

2.16 The proposed Data Portability Obligation will apply to any organisation[6] that collects, uses or discloses personal data in Singapore, except for the following[7]:

(a) Any individual acting in a personal or domestic capacity;

(b) Any employee acting in the course of his or her employment with an organisation;

(c) Any public agency; and

(d) Any organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of personal data.

2.17 The proposed Data Portability Obligation will not apply to a data intermediary[8] in relation to data that it is processing on behalf of and for the purposes of another organisation. PDPC notes that an organisation may engage a data intermediary to carry out processing of data, which could include the transmission of data on behalf of the organisation to fulfil a data portability request. An organisation may enter into a contract with its data intermediary for the latter to assist with processing and responding to a data portability request on its

[6] The PDPA defines an organisation as "any individual, company, association or body of persons, corporate or unincorporated whether or not formed or recognised under the law of Singapore; or resident, or having an office or a place of business, in Singapore".

[7] Section 4(1) of the PDPA.

[8] The PDPA defines a data intermediary as "an organisation that processes personal data on behalf of another organisation but does not include an employee of that other organisation". A data intermediary does not include an employee.

behalf. The organisation that engages the data intermediary remains responsible for ensuring compliance with the proposed Data Portability Obligation under the PDPA.

Receiving organisation

2.18 Organisations will only be required to transmit data to other organisations ("receiving organisations") that have a presence in Singapore[9]. Organisations will not be required, as a matter of compliance with the proposed obligation, to transmit data to overseas receiving organisations. However, this is not intended to prevent voluntary arrangements by organisations to transmit data to overseas organisations with consent of the individual[10].

Requesting individual

2.19 Any individual[11], regardless of whether the individual is in Singapore, may make a data portability request to an organisation that is covered by the proposed Data Portability Obligation.

2.20 An individual who is validly acting on behalf of another individual (e.g. parent or legal guardian acting on behalf of his or her child) may make a request on behalf of that other individual for an organisation to port his or her data. This is consistent with section 14(4) of the PDPA which provides that consent may be given, or deemed to have been given, by any person validly acting on behalf of the individual for the collection, use or disclosure of the individual's personal data. Further clarification will be provided in PDPC's advisory guidelines and additional requirements may be set out in codes of practice on verifying the requesting individual's identity and situations where a person may validly act on behalf of an individual.

Covered data

2.21 Data portability is intended to support the growth of the Digital Economy. Given that digital data is the currency powering the Digital Economy, the ability to move such data within and across sectors is crucial to the growth of the Digital Economy.

2.22 In line with this objective, the PDPC is proposing for the proposed Data Portability Obligation to 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

[9] Such organisations should either be formed or recognised under the law of Singapore; and resident, or having an office or a place of business in Singapore.
[10] Porting of data to overseas organisations must be done in compliance with the Data Protection Provisions, including the Transfer Limitation Obligation.
[11] The PDPA defines an individual as "a natural person, whether living or deceased", and excludes unincorporated groups of individuals such as an association which may take legal action in its own name.

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.

2.23 PDPC recognises the need to distinguish between the different types of data that would be subject to the proposed Data Portability Obligation. This should take into consideration the potential impact to companies' competitive positions and business innovation. Specifically, recognition should be given to the generation of data by virtue of an organisation's innovative product or service offering, and the proprietary input of businesses in deriving new insights.

2.24 In order to reap the maximum benefits for consumers and the economy, PDPC proposes for the Data Portability Obligation to apply to data[12] that is:

(a) provided by the individual to the organisation ("**user provided data**"); and

(b) generated by the individual's activities in using the organisation's product or service ("**user activity data**").

2.25 Examples of **user provided data** include the individual's personal details, contact information, personal preferences and any other information that the individual has provided to the organisation, including information that an individual may have provided to the organisation through a third party. Information in the form of documents, photographs, email messages, social media posts etc, that has been provided by the user is also within the scope of user provided data.

2.26 Examples of **user activity data** include the individual's transactions and purchases, search history, location data, outgoing and incoming call logs, steps count and pulse rate collected through the use of an activity tracker.

2.27 To promote business innovation, PDPC is proposing to provide for a similar exception to the Access Obligation for **data which, if disclosed, would reveal confidential commercial information that could harm the competitive position of the organisation**. This is not intended to affect general competition in the market, but to protect first movers who bring to market an innovative product or service from unfair competition by fast followers. The proposed Data Portability Obligation is not intended to remove the commercial incentives for constant innovation. However, an innovative product or service will become a standard

[12] Not limited to the definition of "personal data" in the PDPA, and does not apply to personal data collected without consent (e.g. where required or authorised under the PDPA or other written law).

feature with the passage of time. The proposed exception to port data that is associated with an innovative product or service should not exempt a first mover for an unnecessarily prolonged period. PDPC would like to seek feedback on the relevant considerations in striking the right balance.

2.28 Recognising that organisations may use data to derive new business insights with business-specific input and such data would be proprietary to these organisations, PDPC proposes to provide an exception to the Data Portability Obligation for "**derived data"**. "Derived data" refers to new data element that is created through the processing[13] of other data by applying business-specific rules (see subsequent section on "derived data" under Part III). Table 1 below provides examples of user provided and user activity data that are subject to the proposed Data Portability Obligation, as well as examples of derived or other data not subject to the proposed Data Portability Obligation.

Table 1: Examples of user provided, user activity and derived data

Type of organisation	**Data subject to Data Portability Obligation**		**Data not subject to Data Portability Obligation**
	User provided data	**User activity data**	**Derived data**
Social media platform	• User's sign up information (e.g. name, email address) • User's profile information (e.g. schools, workplaces, religion, political views) • User's indicated preferences for news feeds/ads	• User's friends/contacts, groups created/joined • User's activities and uploads (e.g. posts, likes, tags, check-ins, comments, posts read, search activities etc)	• Friends suggestions and suggested posts based on analyses of users' profiles, contacts and activities
Public transport service	• Commuter's sign up information (e.g. name, contact details, credit card information)	• Dates, timings and locations of commuter's utilisation of public transport service • Commuter's top-up payments/transactions	• Predicted peak and off-peak travel patterns based on analyses of commuters' travel histories
Hotel	• Guest's registration information (e.g. name, email address, passport number) • Guest's indicated preferences	• Dates of guest's stay • Guest's purchases and transactions (e.g. in-room services)	• Customised packages and reward offers based on analyses of guests' usage and preferences

2.29 While the Data Protection Provisions of the PDPA do not apply to **business contact information (BCI)** [14], it is proposed for such information to be covered under the proposed Data Portability Obligation as BCI is provided by the individual to facilitate business

[13] Processing is to be defined broadly to include the use of any mathematical, logical, statistical, computational, algorithmic, or analytical methods.

[14] Business contact information is defined in the PDPA as "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes".

activities, allowing individuals to port his or her data supports this objective of promoting business activities. For instance, where an individual has provided his or her business contact information (e.g. business email address or business telephone number) to an organisation, that information may be included as part of the data to be ported by the organisation at the individual's request.

2.30 The data is not limited to the personal data of the individual, but 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.

2.31 PDPC takes the view 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.

2.32 Further examples to illustrate the intended scope of coverage of the proposed Data Portability Obligation are provided below.

2.33	**Example** Peter provides his business card to a F&B dining group to sign up for a corporate membership with the F&B dining group. Peter may subsequently request for his data, including his business contact information, collected by the F&B dining group to be ported to another organisation.
2.34	**Example** Tom wishes to sign up with new Electricity Service Provider ABC that has a standing arrangement with Internet Service Provider DEF to roll out a bundled package for new customers. As an existing customer of Internet Service Provider GHI, and to enjoy the promotional offers for the bundled package by ABC and DEF, Tom requests for his personal and transactional data with his existing Internet Service Provider GHI to be ported to new Electricity Service Provider ABC and Internet Service Provider DEF in order to sign up for the bundled package.

	Under the proposed Data Portability Obligation, Internet Service Provider GHI must port Tom's data to Electricity Service Provider ABC and Internet Service Provider DEF.
2.35	**Example** For compliance purposes, casinos are required under the Casino Control Act to collect certain personal data of casino patrons as well as the patron's transactional data. Where organisations are required by law to collect personal data of individuals for compliance purposes, such data would not be subject to the proposed Data Portability Obligation.
2.36	**Example** Mary has applied for a financial assistance grant which is administered by Voluntary Welfare Service (VWO) A. In assessing and evaluating Mary's eligibility for this grant, VWO A collects Mary's personal data from Family Services Centre B, which had previously provided various home care services to Mary, without Mary's consent pursuant to the exception to the consent requirement for collection that is necessary for evaluative purposes under the PDPA. The personal data of Mary collected by VWO A by relying on an applicable exception to the consent requirement under the PDPA would not be subject to the proposed Data Portability Obligation.

Handling data portability requests

2.37 The following sets out the key responsibilities of the porting organisation in receiving and responding to a data porting request under the proposed Data Portability Obligation.

(a) **Receiving the request** – The 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. The individual's request should include sufficient information to identify the individual making the request and the types and amount of data requested for porting.

(b) **Verifying the request** – Upon receiving a data portability request by an individual, the porting organisation must ensure the veracity of the request[15]. For example,

[15] This includes checking the validity of any request by a person acting on an individual's behalf to request for the porting of the individual's data.

this can be achieved by providing the function to request for porting of data after the requesting individual has securely logged into the online service.

(c) **Verifying the data to be ported** – Before 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).

(d) **Porting the data** – 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:

(i) **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 (see subsequent section on power to review); and

(ii) **when the data will be ported** to the receiving organisation. The period from the time the individual requests for the data to be ported to the time the data is ported must be within a reasonable period. PDPC is proposing to prescribe in Regulations a period of no longer than 7 calendar days for the porting of data upon confirmation of the data (or any other periods as specified under the codes of practice).

(e) **Format for porting data** – Given the wide range of types of data that could be processed by organisations, PDPC will not prescribe the data formats that an organisation should adopt for transmitting data. To facilitate interoperability, the formats used should be easily accessible and affordable to any organisation receiving the data. Where possible, open data formats should be used. Formats that are subject to costly licensing agreements, for instance, would not be considered to be acceptable formats.

Porting organisations should provide technical information about the data formats that are used, and protocols for transmitting and receiving the data. While organisations are required to transmit and receive data in a common, machine-readable format, it does not prevent receiving organisations from converting the received data into formats that are used in its product or service.

(f) **Informing the individual of a rejection** - Where the organisation rejects a data porting request (e.g. it does not hold data of the individual that is covered by the requirement, or an exception applies), it must inform the individual as soon as practicable of the rejection and the reason for the rejection.

(g) **Preserving the data** - Organisations will be required to preserve the requested data upon receiving a data porting request by an individual. Where the organisation rejects a data porting request (including when the individual does not agree to pay the fees), the organisation must continue to preserve a copy of the requested data for a reasonable period - minimally 30 calendar days after rejecting the request. This is to allow PDPC to review an organisation's rejection of a data porting request[16]. To be clear, this does not impose an obligation on organisations to retain data just for the purpose of meeting possible data portability requests.

(h) **Withdrawal of request** - The requesting individual may withdraw the request to port his or her data any time before the data is transmitted, in which case the porting organisation must take reasonable steps to cease (and cause its data intermediaries or agents to cease) to transmit the data.

2.38 As a matter of good practice, the porting organisation should check that the data transmitted has been received by the receiving organisation and assist with any queries it may have with regard to the data transmitted.

Receiving ported data

2.39 The receiving organisation should verify the completeness and conformity to formats and standards of data that are transmitted to it by a porting organisation pursuant to a data portability request. Where the data is irrelevant or excessive in relation to the product or service that it provides to the individual, it may choose not to accept the data or to retain only a portion of the data. Ported 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.

[16] In the event the individual submits an application for review to the PDPC and the PDPC determines that it will review the case, as soon as the organisation receives a Notice of Review Application from the PDPC, it should continue to preserve the requested data until the review by PDPC is concluded and any right of the individual to apply for reconsideration and appeal is exhausted.

2.40 For instance, the recipient organisation must inform the individual the purposes for which it is collecting, using and disclosing the ported data, and ensure that consent is obtained from the individual for these purposes.

2.41 Where the recipient organisation encounters issues accessing the transmitted data (e.g. incomplete transmission or corruption of data during transmission), the receiving organisation should contact the porting organisation. Notwithstanding, should the porting organisation fail to transmit the data in accordance with the proposed Data Portability Obligation, the receiving organisation or the individual may submit an application to the PDPC for a review. (See subsequent section on power to review.)

Alignment with Access Obligation

2.42 Currently, the PDPA already provides for the right of individuals to request for access to their personal data in the possession or under the control of the organisation, and organisations have the obligation to provide the requested personal data ("Access Obligation")[17]. The objective of the Access Obligation is to protect individuals' interests by making organisations accountable to individuals for the personal data they hold of them. As the Access Obligation covers personal data collected from sources other than the individual, the individual is able to verify all personal data the organisation has of them, and the ways in which the organisation has been using his or her personal data. Similarly, the objective of data portability is to provide individuals with greater control over their data by having the ability to move their data to another organisation and benefit from greater choice in products and service offerings.

2.43 The proposed Data Portability Obligation is complementary to the Access Obligation by extending the ability of individuals to access their personal data held by an organisation, to the ability to transmit their data to another organisation. While data portability applies only to electronic data provided or generated by the individual in using a product or service, this is complemented by the Access Obligation which allows individuals to access or obtain a copy of his personal data (including those held in non-electronic form).

2.44 PDPC proposes to provide for **similar exceptions** to the Data Portability Obligation as the current exceptions to the Access Obligation[18]. The intent is to ensure that where an organisation is not required to provide access to a requesting individual's personal data pursuant to section 21 of the PDPA, the organisation will also not be required to provide the individual access to or a copy of the data for porting to another organisation pursuant to the Data Portability Obligation. Annex A provides an overview of the Access Obligation

[17] Section 21 of the PDPA.
[18] Fifth Schedule to the PDPA.

and the proposed Data Portability Obligation, and Annex B provides a comparison of the exceptions to the Access Obligation and the proposed exceptions to the Data Portability Obligation.

2.45 Exceptions to the Data Portability Obligation will be aligned to exceptions to Access Obligation except for the prohibitions provided for situations where it could (i) reveal personal data about another individual[19]; or (ii) reveal the identity of the individual who has provided the personal data and that individual does not consent to the disclosure of his identity[20]. This is because the proposed Data Portability Obligation is intended to enable the porting of data provided by the individual, or generated by the individual's activities in using the product or service, and such data may include the personal data of other individuals (e.g. an individual's contact lists and photos of other individuals, email or instant messaging communications with other individuals).

2.46 Given that such data will be accessible to the individual via the proposed Data Portability Obligation, PDPC proposes to limit the additional prohibitions under the Access Obligation (i.e. where it could (i) reveal personal data about another individual; or (ii) reveal the identity of the individual who has provided the personal and that individual does not consent to the disclosure of his identity) only to personal data about other individuals not provided by the individual or generated by the individual's activities in using the product or service. This is to ensure better alignment between the scope of data that organisations may provide to individuals under the Access Obligation and the proposed Data Portability Obligation.

Power to review

2.47 In terms of enforcement, the PDPA will provide for PDPC's **powers to review an organisation's: (i) refusal to port data; (ii) failure to port data within a reasonable time; and, (iii) fees for porting data, pursuant to an individual's data portability request**[21]. This would provide the necessary regulatory safeguards and recourse to protect consumers in the exercise of their right to data portability. The breach of the Data Portability Obligation would be subject to the same penalty framework as a breach of the Data Protection Provisions under the PDPA. Upon completion of review, PDPC may uphold an organisation's refusal to port data or fees charged (e.g. where the organisation has relied on an applicable exception[22] such that it need not port the data), or direct the organisation

[19] Section 21(3)(c) of the PDPA.
[20] Section 21(3)(d) of the PDPA.
[21] This is similar to the powers to review for the Access Obligation provided for under the PDPA today. Under section 28 of the PDPA, PDPC may, upon the application of an individual, review a refusal to provide access to personal data, a failure to provide such access within a reasonable time, or a fee required by the organisation.
[22] MCI and PDPC also intend to provide for exclusions and exceptions to the proposed Data Portability Obligation, similar to those provided for the Access Obligation under the current PDPA (see paragraph 2.44).

to port the data if its reasons for refusing are unfounded, or to reduce the fees charged if they are assessed to be not reasonable.

2.48 Additionally, PDPC will be empowered to direct a porting organisation to suspend transmission of data in certain circumstances where porting of data may not be desirable, such as where there are counterparty risks involved (e.g. fraudulent activity).

Codes of practice

2.49 PDPC recognises that certain industries and sectors may have more specific requirements and standards for the porting of data requested by individuals. PDPC is thus proposing to **introduce the power for PDPC to prescribe binding codes of practices for data portability that may apply to organisations in specific clusters or sectors**. The proposed codes of practices will be issued as subsidiary legislation under the PDPA and will be legally binding. PDPC intends to develop these codes of practice in consultation with the relevant sector regulators and industry stakeholders. Matters to be prescribed under the proposed sectoral codes of practices will include the following:

a) **Consumer safeguards:** information that organisations would need to provide to consumers to enable them to exercise their right to data portability and for their protection (e.g. "cooling off" period[23], opportunity to view the data or sample of the data before it is transmitted);

b) **Counterparty assurance:** criteria for participation and measures to verify the identity of the receiving organisation prior to transmission of data to guard against fraud;

c) **Interoperability**: minimum, open or common machine-readable formats and standards for transmission of data between organisations; and,

d) **Security of data**: minimum standards to ensure the protection of data during transmission and the integrity and security of participating systems.

[23] In appropriate situations, a "cooling off" period may be provided for the individual to change his or her mind to port his or her data to the receiving organisation.

Questions:

Q1. What are your views on the impact of data portability, specifically on consumers, market and economy?

Q2. What are your views on the proposed Data Portability Obligation, specifically –

- ***a) scope of organisations covered; and***
- ***b) scope of data covered?***

Q3. What are your views on the proposed exceptions to the Data Portability Obligation, specifically –

- ***a) the proposed exception relating to 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***
- ***b) the proposed exception for "derived data"?***

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

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?

Q6. 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?

PART III: PROPOSED DATA INNOVATION PROVISIONS

3.1 The modern business marketplace is very much a data-driven environment, where data is at the core of almost every business decision made. Examples include the use of data to identify target audience, or customise new products or services to cater to the individual needs or segments of the market.

3.2 PDPC recognises that there is a need to support data-driven innovation and facilitate organisations' use of data to better understand their customers, make informed business decisions in relation to product and service development and optimise operational efficiencies. Consequently, consumers will benefit through more relevant and personalised services offered by organisations. However, the industry's feedback has been that there is uncertainty over whether consent is necessary in order to use personal data for such purposes, if no exceptions to the consent requirement apply. PDPC hence intends to make clear in the PDPA how organisations may use data for appropriate purposes, so as to provide organisations with confidence to harness the data they hold for business innovation.

A. Business Innovation Purposes

3.3 To enable organisations to confidently use data to derive business insights and innovate in the development and delivery of products and services, PDPC intends to introduce provisions in the PDPA to clarify that organisations can use personal data (collected in compliance with the Data Protection Provisions of the PDPA) for the purposes ("business innovation purposes") of:

(i) operational efficiency and service improvements;
(ii) product and service development; or
(iii) knowing customers better.

3.4 The following paragraphs set out how specific Data Protection Provisions are envisaged to apply to business innovation purposes.

Consent and Notification Obligations

3.5 PDPC intends to clarify 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.

3.6 To be clear, this proposed provision for business innovation purposes does not extend to the use of data for sending direct marketing messages to customers. Organisations must obtain consent for the sending of such direct marketing messages to individuals. For example, an organisation may use a customer's personal data without consent for the data innovation purpose of product and service development, but may only send the customer direct marketing messages about the new product if it has obtained consent from the customer for receiving such marketing messages.

3.7 Where individuals withdraw their consent for the use or disclosure of their personal data for the purposes for which the organisation had collected the personal data, organisations may continue to use such personal data for business innovation purposes.

3.8	**Example** Credit card company ABC uses its customers' personal data (i.e. credit payment history) to derive insights on spending habits of its customers, and to develop its new credit card package. In doing so, derived personal data such as ABC's categorisation of customers' financial health and spending propensity is created. ABC's use of personal data for the creation of derived personal data can be done without consent as it falls within the scope of business innovation purposes. ABC intends to use the derived personal data consisting of its categorisation of customers' financial health to conduct further analysis on the target audience and to design its new credit card rewards scheme. In this case, ABC is not required to obtain consent to use such derived personal data as the use is for business innovation purposes. ABC intends to disclose the derived personal data consisting of customers' spending propensity to Shopping Mall DEF, for DEF to know its customers better. In this case, ABC is required to obtain consent to disclose the derived personal data to DEF, as the proposed provision for business innovation purposes only applies to the use of personal data.

Retention for business innovation purposes

3.9 Under the PDPA, an organisation must cease the retention of documents containing personal data or remove the means by which personal data can be associated with particular individuals (e.g. by anonymisation) once the purposes for which the personal data was collected are no longer being served by retention of the personal data, and retention is no longer necessary for legal or business purposes ("Retention Limitation Obligation")[24].

[24] Section 25 of the PDPA.

3.10 In addition, PDPC proposes to clarify that the business innovation purposes specified in paragraph 3.3 will be considered business purposes for which retention of the personal data may be necessary. If any individual withdraws consent for the purposes of the collection, use or disclosure of his or her personal data, the organisation must ensure that the individual's personal data, including any derived personal data, is retained only for so long as it is necessary for a legal or business purpose.

3.11 Organisations should have in place appropriate retention policies which set out their approach to retention periods for personal data, taking into consideration the risks of any unauthorised access or disclosure of personal data in their possession or under their control.

B. Derived data

3.12 Organisations may process personal data to derive new insights and information[25]. PDPC refers to new data that is created through the processing[26] of other data by applying business-specific logic or rules as "derived data". Depending on the business-specific rules applied, derived data may still be capable of identifying an individual ("derived personal data"). PDPC notes that it would be important to recognise the business-specific input and processing by an organisation in deriving new data and information, and to make a distinction between the rights of individuals and organisations in respect of derived personal data.

3.13 Derived personal data enriches the information that an organisation has about an individual. Where personal data is used for the creation of derived personal data for business innovation purposes (i.e. for operational efficiency and service improvements; product and service development; or knowing customers better), organisations will not be required to notify the individual and obtain consent to do so. Consent is also not required to use the derived personal data for business innovation purposes. (See section on business innovation purposes above.)

3.14 PDPC proposes to provide that derived personal data will <u>not</u> be subject to the following obligations under the PDPA:

(i) Access Obligation[27];

(ii) Correction Obligation; and

[25] The resultant data may or may not relate to an identifiable individual. Where the derived data can identify an individual, it is derived personal data. Where it cannot identify an individual, such derived data is not considered personal data, and the Data Protection Provisions of the PDPA would not apply to its collection, use or disclosure.
[26] Processing is to be defined broadly to include the use of any mathematical, logical, statistical, computational, algorithmic, or analytical methods.
[27] Section 21(1)(a) of the PDPA.

(iii) Proposed Data Portability Obligation (refer to Part II).

3.15 Where an individual cannot be identified from the derived data, or from that data and other information to which the organisation has or is likely to have access, it is not personal data and the Data Protection Provisions of the PDPA do not apply to the collection, use or disclosure of such data.

Access and correction of derived personal data

3.16 Under the Access Obligation[28], upon an individual's request, an organisation is required to provide the individual with (i) personal data about the individual that is in the possession or under the control of the organisation, and (ii) information about the ways in which the personal data has been or may have been used or disclosed by the organisation within a year before the date of the request. In addition, under the Correction Obligation[29], individuals may submit a correction request to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organisation, and organisations are to correct the personal data in question.

3.17 PDPC intends to provide that organisations need not, upon the individual's request, provide the individual with derived personal data, nor correct derived personal data about the individual that is in the possession or under the control of the organisation. This is in view that derived data is obtained through the business-specific input and processing of data by an organisation, and that there may be potential commercial and business sensitivities if requests for access to or correction of such data were to be granted.

3.18 While organisations are not required to provide individuals with access to derived personal data, organisations will nevertheless be required to provide the individual information about the ways in which the derived personal data has been or may have been used or disclosed by the organisation within a year before the date of the request[30]. In doing so, the organisation may develop a standard list of all possible third parties to whom the derived personal data may be disclosed, and provide information on the purposes rather than the specific activities for which the derived personal data had been or may have been used or disclosed.

3.19 Where an individual requests to correct an error or omission in his or her personal data, the organisation is required to make that correction, and where appropriate, this extends to any personal data used to create the derived data so as to ensure accuracy of the data

[28] Section 21 of the PDPA.
[29] Section 22 of the PDPA.
[30] Section 21(1)(b) of the PDPA.

held by the organisation. However, the organisation need not accede to requests from individuals to correct the derived personal data.

Application of other Data Protection Provisions to derived personal data

3.20 Other than the Access and Correction Obligations and the proposed Data Portability Obligation that will not apply to derived personal data, organisations would still be required to comply with all other Data Protection Provisions of the PDPA in respect of derived personal data.

3.21 Specifically, organisations are required to make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data is (i) likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or (ii) likely to be disclosed by the organisation to another organisation ("Accuracy Obligation"). Organisations must therefore make a reasonable effort to ensure that the derived personal data is accurate and complete if it is likely to be used to make a decision that affects the individual, or to be disclosed to another organisation.

Questions:

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?

Q8. What are your views on the proposed definition of "derived data"?

Q9. What are your views on the proposal for the Access, Correction and proposed Data Portability Obligations not to apply to derived personal data?

PART IV: SUBMISSION OF COMMENTS

4.1 Parties that wish to submit comments on this public consultation paper should organise their submissions as follows:

a) cover page (including particulars of the organisation and contact person);

b) comments, with reference to specific sections or paragraphs if appropriate; and

c) conclusion.

4.2 Supporting material may be placed in an annex. All submissions should be clearly and concisely written, and should provide a reasoned explanation for any comments.

4.3 Where feasible, parties should identify the specific section on which they are commenting and explain the basis for their proposals.

4.4 All submissions should reach PDPC by **17 July 2019**. Comments should be submitted:

a) in soft copy (in Microsoft Word format);

b) to the following e-mail address: corporate@pdpc.gov.sg; and

c) with the email header: "PDPC's Public Consultation on Proposed Data Portability and Data Innovation Provisions".

4.5 PDPC reserves the right to make public all or parts of any written submission and to disclose the identity of the source. Commenting parties may request confidential treatment for any part of the submission that the commenting party believes to be proprietary, confidential or commercially sensitive. Any such information should be clearly marked and placed in a separate annex. If PDPC grants confidential treatment, it will consider, but will not publicly disclose, the information. If PDPC rejects the request for confidential treatment, it will return the information to the party that submitted it and will not consider this information as part of its review. As far as possible, parties should limit any request for confidential treatment of information submitted. PDPC will not accept any submission that requests confidential treatment of all, or a substantial part, of the submission.

END OF DOCUMENT

ANNEX A

COMPARISION OF ACCESS OBLIGATION AND PROPOSED DATA PORTABILITY OBLIGATION

	Access Obligation	Proposed Data Portability Obligation
When it is activated	• Upon request of the individual	• Upon request of the individual
Who the data is provided to	• The individual	• The individual and the receiving organisation specified by the individual
Scope of data	• Personal data of the individual in the possession or under the control of the organisation • Information about the ways in which the personal data has been used or disclosed by the organisation (within a year before the date of request)	• User provided data (i.e. data that was provided to the organisation by the individual) • User activity data (i.e. data generated by the individual's activities or usage of a product or service) • Not limited to personal data of the individual, may include data about another individual • Does not apply to data collected without consent or where required or authorised under the PDPA or other written law • Does not apply to derived data, and data which, if disclosed, could harm the competitive position of the organisation

Prohibitions	• Threaten the safety or physical/mental health of another individual • Cause immediate or grave harm to the safety or to the physical/mental health of the requesting individual • Contrary to the national interest • Reveal personal data about another individual* • Reveal the identity of an individual who has provided the personal data, and that individual does not consent to the disclosure of his identity* ** PDPC proposes to scope these prohibitions to personal data not provided or generated by the individual's activities in using the product or service*	• Threaten the safety or physical/mental health of another individual • Cause immediate or grave harm to the safety or to the physical/mental health of the requesting individual • Contrary to the national interest
Format of data	Personal data held in physical, electronic or documentary form[31]	Data held in electronic form
Preservation of requested data	Organisation is required to keep the requested data minimally for 30 calendar days after rejecting the request	Organisation is required to keep the requested data minimally for 30 calendar days after rejecting the request
Time period for responding	Organisation must provide access as soon as reasonably practicable from the time the access request is received 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	Organisation must port the data as soon as reasonably practicable from the time it receives the individual's request to port data. Organisation should port the data within 7 calendar days, or any other periods as specified under the codes of practice

[31] If the requested data resides in a form that cannot practicably be provided to the individual in documentary form, whether as physical or electronic copies (e.g. the data cannot be extracted from a special machine owned by the organisation), then the organisation may provide the individual a reasonable opportunity to examine the requested data in person.

Charging of fees	Organisation may charge the individual a reasonable fee for access request	Organisation may charge the individual or the receiving organisation a reasonable fee for data portability request
PDPC's powers	• Power to review organisation's a) refusal to provide access to personal data b) failure to provide such access within a reasonable time c) fees for data access request • Upon completion of review, PDPC may a) uphold a refusal or direct the organisation to provide access b) confirm, reduce or disallow a fee, or direct the organisation to make a refund	• Power to review organisation's a) refusal to port data b) failure to port data within a reasonable time c) fees for data portability request • Upon completion of review, PDPC may a) uphold a refusal or direct the organisation to port the data b) confirm, reduce or disallow a fee, or direct the organisation to make a refund • Power to direct the organisation to suspend porting • Power to prescribe legally binding codes of practice that apply to specific clusters/sectors

ANNEX B

EXCEPTIONS TO ACCESS OBLIGATION AND PROPOSED EXCEPTIONS TO DATA PORTABILITY OBLIGATION

Exceptions to Access Obligation	Proposed exceptions to Data Portability Obligation
• derived data* ** PDPC proposes to provide an exception to section 21(1)(a) for derived data*	• derived data
• opinion data[32]	• opinion data
• any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results	• any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results
• personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust	• personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust
• personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre	• personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre
• a document related to a prosecution if all proceedings related to the prosecution have not been completed	• a document related to a prosecution if all proceedings related to the prosecution have not been completed
• personal data which is subject to legal privilege	• personal data which is subject to legal privilege
• personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation	• data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation
• personal data collected, used or disclosed without consent, under paragraph 1(e) of the Second Schedule, paragraph 1(e) of the Third Schedule or paragraph 1(f) of the Fourth Schedule, respectively, for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed	• personal data collected without consent under the Second Schedule (i.e. all exceptions to the consent requirement)
• personal data was collected or created by a mediator or arbitrator in the conduct of a	• personal data was collected or created by a mediator or arbitrator in the conduct of a

[32] PDPC is proposing to broaden the current exception for opinion data kept solely for an evaluative purpose, to any opinion data. The proposed exception for any opinion data will also be provided for the proposed Data Portability Obligation.

mediation or arbitration for which he was appointed to act (i) under a collective agreement under the Industrial Relations Act (Cap. 136) or by agreement between the parties to the mediation or arbitration; (ii) under any written law; or (iii) by a court, arbitral institution or mediation centre	mediation or arbitration for which he was appointed to act (i) under a collective agreement under the Industrial Relations Act (Cap. 136) or by agreement between the parties to the mediation or arbitration; (ii) under any written law; or (iii) by a court, arbitral institution or mediation centre
• any request – (i) that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests; (ii) if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests; (iii) for information that does not exist or cannot be found; (iv) for information that is trivial; or (v) that is otherwise frivolous or vexatious.	• any request – (i) that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests; (ii) if the burden or expense of providing access to and/or porting the requested data would be unreasonable to the organisation or disproportionate to the individual's interests; (iii) for information that does not exist or cannot be found; (iv) for information that is trivial; or (v) that is otherwise frivolous or vexatious.