SINGAPORE EXCHANGE LIMITED'S COMMENTS ON THE PUBLIC CONSULTATION ON REVIEW OF THE PERSONAL DATA PROTECTION ACT 2012 – PROPOSED DATA PORTABILITY AND DATA INNOVATION PROVISIONS

17 July 2019

Submitted by: Singapore Exchange Limited
2 Shenton Way, #02-02
SGX Centre 1
Singapore 068804

SINGAPORE EXCHANGE LIMITED'S COMMENTS ON THE PUBLIC CONSULTATION ON REVIEW OF THE PERSONAL DATA PROTECTION ACT 2012 – PROPOSED DATA PORTABILITY AND DATA INNOVATION PROVISIONS

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

1 Nil.

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

a) scope of organisations covered; and

b) scope of data covered?

Scope of organisations

2.1 We welcome the following proposals:

(a) that the scope of organisations covered should be consistent with the existing scope of the Act, and that the carve-outs under section 4(1) of the Personal Data Protection Act 2012 ("**PDPA**") should similarly apply to the Data Portability Obligation (paragraph 2.16);

(b) that the Data Portability Obligation should not apply to a Data Intermediary in relation to the data that it is processing on behalf of and for the purposes of another Covered Organisation (paragraph 2.17); and

(c) that Covered Organisations should only be required to transmit personal data to Receiving Organisations that have a presence in Singapore (paragraph 2.18).

Covered Organisations to have directly collected personal data from individuals

2.2 In addition, in relation to 2.1(b) above, we suggest that **the Data Portability Obligation also clearly state that a Requesting Individual may only make a request to a Covered Organisation which directly collected personal data from that Requesting Individual**.

2.3 This suggestion is based on the following considerations:

(a) First, this is a logical consequence in accordance with the clarification that the Data Portability Obligation will not apply to a Data Intermediary in relation to data that it is processing on behalf of and for the purpose of another organisation: *i.e.* an organisation other than the Covered Organisation which directly collected personal data from the Requesting Individual is a data intermediary *vis-à-vis* that Requesting Individual.

(b) Second, only a Covered Organisation which directly collected personal data from the Requesting Individual is able to accurately determine whether a specific piece of data is User Provided Data, User Activity Data *or* Derived Data to be ported or not ported, as the case may be.

(c) Third, by allowing a Requesting Individual to make data portability requests to an organisation other than the Covered Organisation which directly collected personal data from that Requesting Individual may result in a circumvention of that Covered Organisation's right to rely on applicable exceptions, *e.g.* in relation to the Covered Organisation's confidential commercial information on that Requesting Individual which, if disclosed, could harm the competitive position of that Covered Organisation.

(d) Fourth, by allowing a Requesting Individual to make data portability requests to an organisation other than a Covered Organisation which directly collected personal data from that Requesting Individual would result in undue additional compliance costs, including time and effort to verify the identity of the Requesting Individual, the authenticity and nature of the request and scope of personal data involved, *etc*., before execution of said request.

2.4 We note that the feedback above is consistent with the right of data portability under Article 20(1) of the General Data Protection Regulation ("**GDPR**"), which reads:

> "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: …"
>
> [emphasis added]

2.5 In addition, Recital 68 to the GDPR further clarified that: "[The right to data portability] should not apply where processing is based on a legal ground other than consent or contract."

2.6 This requirement to data portability is similarly entrenched in the United Kingdom ("**UK**"). We note from UK Information Commissioner's Office's ("**ICO's**") guidance on data portability, which clarified on its website (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/) that:

> "**When does the right apply?**
>
> The right to data portability only applies when:
>
> - your lawful basis for processing this information is consent **or** for the performance of a contract; and
>
> - you are carrying out the processing by automated means (i.e. excluding paper files)."

2.7 We propose that the same requirement be clearly articulated in our Data Portability Obligation, such that it is clear that a Requesting Individual may only make a request to a Covered Organisation which directly collected personal data from that Requesting Individual.

Covered Organisations and Receiving Organisations to be offering similar services

2.8 In addition to 2.1(c) above, we suggest that **the Data Portability Obligation provides that a Covered Organisation should only be required to transmit personal data to a Receiving Organisation offering similar services as the Covered Organisation**. This is so as different types of service providers will collect different types of data from the same individual, *e.g.* the data set collected by a tele-communications service provider will differ from that collected by a credit card-issuing bank. This would result in not-fit-for-purpose data sets, and Requesting Individuals would still have to provide additional information to the Receiving Organisations directly notwithstanding the ported data. Accordingly, data portability between different types of service providers would not result in sufficient benefits to outweigh the compliance costs.

2.9 For the above stated reasons, we are of the view that the Data Portability Obligation would only yield sufficient value and outweigh the additional compliance costs when the Covered Organisations and Receiving Organisations are offering the same type of services.

Scope of data covered

2.10 We agree with the following proposals:

(a) that the proposed Data Portability Obligation apply only to personal data in the possession or control of organisations that is held in electronic form;

(b) that the scope of data comprises User Provided Data and User Activity Data;

(c) that an exception be provided for personal data which, if disclosed, would reveal confidential commercial information that could harm the competitive position of the organisation; and

(d) that an exception be provided for Derived Data.

2.11 We are of the view that the following should fall outside the scope of data covered by the Data Portability Obligation:

(a) Personal data of third parties. We note that it would be operationally difficult for a Covered Organisation to process a data portability request by a Requesting Individual involving personal data of third parties, as it would require:

(i) the Covered Organisation to distinguish between personal data provided on a first-person basis from the third party and third-person basis from the Requesting Individual, as only the latter would be within scope of the data portability request;

(ii) the Covered Organisation to verify whether the request by the Requesting Individual is inconsistent with the consent of the person to which the personal data relates, when the same piece of personal data had been provided by both the Requesting Individual and the person; and

(iii) the Covered Organisation to verify with the person to which the personal data relates whether the Requesting Individual was duly authorised to make the data portability request on behalf of said person.

(b) Conflict with any other legal or regulatory obligation. We are of the view that for the avoidance of doubt section 4(6) of the Personal Data Protection Act 2012 should be revised to include reference to the Data Portability Obligation as well. In addition, given that certain Covered Organisations may be concurrently regulated by foreign regulatory authorities, we suggest that a carve-out be similarly provided to address any potential conflicts between the Data Portability Obligation and any regulatory obligations which such Covered Organisations may be subject to.

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"?

Proposed exception relating to commercial confidential information

3.1 We welcome the proposed exception relating to commercial confidential information that could harm the competitive position of organisations.

3.2 However, as what constitutes commercial confidential information may vary greatly between different businesses, we are of the view that the Data Portability Obligation should recognise reasonable flexibility for each business to determine what constitutes its commercial confidential information.

Proposed exception for derived data

3.3 We welcome the proposed exception that Derived Data should fall outside the scope of the Data Portability Obligation. For completeness, please see paragraph 8.2 for additional comments in relation to the proposed definition of Derived Data.

Proposed similar exceptions as the Access Obligation

3.4 We welcome the proposal to provide for similar exceptions to the Data Portability Obligation as the current exceptions to the Access Obligation, *i.e.* the Fifth Schedule to the PDPA.

3.5 In addition, we propose that the Data Protection Obligation provide that the porting of data shall also be subject to a reasonable "technically feasible" limitation. We note from Article 20(2) of the GDPR this limitation, which reads:

> "In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible."
>
> [emphasis added]

3.6 Recital 68 to the GDPR clarified the obligation under this article as follows: "The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible."

3.7 This limitation has been adapted by the UK ICO, which provided the following guidance at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/:

> "You should consider the technical feasibility of a transmission on a request by request basis. The right to data portability does not create an obligation for you to adopt or maintain processing systems which are technically compatible with those of other organisations (GDPR Recital 68). However, you should take a reasonable approach, and this should not generally create a barrier to transmission."

3.8 In similar vein, we propose that the Data Protection Obligation clarifies that technical feasibility is a valid consideration, and where it is reasonably unfeasible to do so a Covered Organisation may reject a request on that basis.

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

4.1 We have the following views in relation to the proposed requirements for handling data portability requests:

(a) Verifying the request. As proposed in paragraph 2.11(a) above, a Requesting Individual should not be allowed to make data portability request in relation to personal data of third parties. In order to sufficiently verify the authenticity of such a request, a Covered Organisation would likely have to reach out to all third parties. As a Covered Organisation may not have direct relationships with those third parties, it may not have the requisite information available to conduct such verifications. In addition, such verifications may not be well received by those third parties. Alternatively, if data portability requests in relation to personal data of third parties are allowed, the Data Portability Obligation should

provide that the Requesting Individual shall indemnify the Covered Organisation in the event any third party disputes the authenticity of the request.

(b) Verifying the data to be ported. While we agree with the proposal for the Requesting Individual to view the data before transmitting it to the Receiving Organisation, we suggest that a Requesting Individual should not be allowed to remove data that falls within the scope of the request but that he / she does not wish to port. This is for the following reasons:

(i) The compliance costs would rise exponentially for Covered Organisations to cater for Requesting Individuals tailoring their personal data for transmission to Receiving Organisations.

(ii) From a Receiving Organisation's perspective, it is not beneficial for Requesting Individuals to be able to cherry pick the transmitted data, as that may enable Requesting Individuals to intentionally remove incriminatory or negative information. It would be beneficial for a Receiving Organisation to receive the entire set of information from an independent Covered Organisation, so as to be in a position to make an objective assessment of the Requesting Individual.

(c) Receiving ported data. We are of the view that it would not be practicable for Receiving Organisations to choose not to accept the data, particularly when such data may be transmitted via email correspondence. To that end, we are of the view that the practical solution would be for the Data Portability Obligation to require:

(i) Requesting Individuals to scope their data portability requests appropriately; and

(ii) Receiving Organisations to confirm to the Requesting Individuals the portion of the ported data which the Receiving Organisations retain, and that the irrelevant data had been deleted accordingly.

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?

5.1 We agree with the proposed powers for the PDPC to review a Covered 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?

6.1 We welcome the proposed binding codes of practices which would be helpful for Covered Organisations. We urge the PDPC to develop such codes of practices in consultation with the relevant sector regulators and industry stakeholders, so as to ensure that the codes of practices are relevant and addresses the specific challenges of each industry.

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?

7.1 We welcome PDPC's proposal to allow organisations to use personal data for business innovation purposes, without the need to notify and seek consent (the "**Data Innovation Proposal**").

7.2 We expect that the Data Innovation Proposal will, if implemented, provide organisations with greater clarity on when and how they will be able to use personal data collected from their customers, in the absence of notification and consent for such use.

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

8.1 We are of the view that the proposed definition of "derived data" must be sufficiently clear, broad-based and unambiguous.

8.2. To this end, we note that the proposed definition of "derived data" is "*new data that is created through the **processing** of other data by applying **business-specific** logic or rules*" (***emphasis*** ours). We make the following suggestions:

(a) "Processing"

We are in favour of the adoption of a broad and flexible definition of "processing" to give effect to the various methods that organisations may adopt in its use of personal data. In this regard, we note that PDPC proposes that "processing" be defined broadly to include the use of any mathematical, logical, statistical, computational, algorithmic or analytical methods. We have several comments on this:

(i) If PDPC intends to adopt the term "processing" in its proposed definition of "derived data", a clear distinction would need to be made against the current definition of "processing" under the PDPA.

(ii) The current definition of "processing" is not suitable for use in the context of "derived data" as it refers to "*the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following…(a) **recording**, (b) **holding**…*" [***emphasis*** ours].

The non-exhaustive list of actions that may fall within the ambit of "processing" such as recording and holding of personal data cannot be a form of "processing" of personal data for the purposes of "derived data" as this would otherwise allow organisations to circumvent the notification and consent requirements, by, for instance, suggesting that the act of "holding" personal data is a means of "processing" personal data for the purposes of obtaining "derived data".

(iii) We note that PDPC's current proposed definition suggests that there must be some degree of automated, technical or mechanical process in order for the output data to fall within the ambit of "derived data". If a new definition of "processing" is introduced for the purposes of the Data Innovation Proposal, we suggest that the definition clarify that "processing" is not limited to mechanical or automated processes. Some guidance may be taken from Article 4(2) of the GDPR which defines processing as:

"*…any operation or set of operations which is performed on personal data or on sets of personal data**, whether or not by automated means,** such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission…"* [***emphasis*** ours].

(b) <u>"Business-Specific"</u>

We are of the view that limiting the scope of "derived data" to cases where an individual's personal data is processed through business-specific logic or rules may be too narrow a construct. We suggest that PDPC consider removing the "business-specific" qualifier or, in the alternative, provide clarity and provide some guidance as to the scope of what would constitute "business-specific", taking into consideration the following:

(i) the introduction of a "business-specific" requirement should not require the means of processing to be unique or exclusive to a particular industry or sector, having regard to the fact that organisations will use varying methods to process personal data, some of which may or may not be business-specific; and

(ii) affected individuals are less likely to be concerned with the means by which their personal data has been processed (i.e. whether it is through a business-specific method or otherwise) than the purposes for which their personal data (and the derived personal data) has been used and the safeguards that are in place to protect such personal data.

(c) <u>Suggestion</u>

In light of our comments above, PDPC could consider defining "derived data" as "*new data that is created by or derived or obtained from the application of a set of logic or rules to personal data, whether or not by automated means*".

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

9.1 We welcome PDPC's proposal that the Access, Correction and proposed Data Portability Obligations will not apply to derived personal data.

9.2 With respect to PDPC's proposal to require organisations to provide an individual information about the ways in which the derived personal data has been or may have been used, we suggest that:

(a) a similar exception as that proposed under the Data Portability Obligation, i.e. for information which, if disclosed, would reveal confidential commercial information that could harm the competitive position of the organisation, be adopted (the "**Exception**") in respect of the requirement to provide information; and

(b) an organisation be provided some flexibility in the form and extent to which it complies with this disclosure requirement (*i.e.* remove any prescriptive requirement to develop standard lists of possible third parties to whom the derived personal data may be disclosed, etc.).

9.3 The reasons for our view are as follows:

(a) Organisations may have legitimate commercial reasons for non-disclosure. As the Data Innovation Proposal is intended to provide flexibility to organisations on how they can use personal data and to encourage business innovation, a specific disclosure obligation (including the provision of a list of possible third parties to whom the derived personal data may be disclosed to) may be counterproductive and discourage innovation, as organisations may have genuine and legitimate commercial reasons as to why certain information (including the way in which derived personal data is used) should not be divulged.

(b) Consistency with the Data Portability Obligation. As the Access Obligations will not apply to derived personal data, an organisation will, correspondingly, not be entitled to rely on the exceptions from the access requirements (as set out in the Fifth Schedule of the PDPA) and, in particular, paragraph 1(g) of the Fifth Schedule of the PDPA, which provides for the Exception.

The introduction of the Exception would be consistent with that under the Data Portability Obligation and provide organisations with some discretion to refuse disclosure where there are compelling commercial reasons to do so. This would also ensure that an organisation is not worse off than if the Access Obligation had applied to derived personal data, in the first instance.

In this regard, the PDPC may also wish to consider stipulating that the exceptions under the Fifth Schedule should likewise be adopted as exceptions to any proposed disclosure requirement. This would be consistent with the Data Portability Obligation and the non-applicability of the Access Obligations to derived personal data.

(c) Existing safeguards under the PDPA continue to apply to derived personal data. There is little room for organisations to abuse the use of derived personal data as the other provisions of the PDPA continue to be applicable vis-à-vis derived personal data. In particular, an organisation remains responsible to ensure its compliance with Part VI of the PDPA which deals with care of personal data. For instance:

(i) Section 23 of the PDPA requires the organisation to make reasonable efforts to ensure that the personal data collected (including the derived personal data) is accurate and complete, where the personal data is, amongst others, likely to be used to make a decision that affects that individual;

(ii) Section 24 of the PDPA requires the organisation to protect the personal data in its possession (which will include the derived personal data) by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(iii) Section 26 of the PDPA requires that an organisation ensure that, in respect of transfers of personal data (including derived personal data) outside Singapore, the receiving organisations are to provide a standard of protection to personal data comparable to that under the PDPA.