XFERS PTE. LTD.
(Incorporated in Singapore)
Co. Reg. No.: 201411660R

17 July 2019

To: Personal Data Protection Commission Singapore
corporate@pdpc.gov.sg

Dear Sir / Mdm,

Xfers Pte Ltd response to PDPC's Public Consultation on Proposed Data Portability and Data Innovation Provisions

1. We thank you for the opportunity to submit our feedback and comments to your public consultation on the proposed data portability and data innovation provisions. Please find our comments and responses set out in the following pages.

2. By way of background, Xfers is an online payment processor and e-wallet provider enabling digital businesses to easily collect from consumers. We are an MAS-approved Widely Accepted Stored Value Facility (https://www.mas.gov.sg/regulation/payments/stored-value-facilities), alongside EZ-Link, NETS Cashcard, NETS Flashpay and CapitaVoucher.

3. Overall, we are very supportive of data portability and we see it as a logical extension to individual's right to access their personal data and increasing interoperability in the digital economy.

4. As a matter of principle, we support this trend of data portability and interoperability because it encourages digital transactions and reduces customer friction. We see interoperability trend already happening in the payments space – where MAS is seeking to alleviate e-wallets and payment networks fragmentation by building interoperability requirements for payment service providers.

5. We look forward to your favourable response to our comments.

Yours faithfully,

Samson Leo

Singapore: *71 Ayer Rajah Crescent, #03-14, Singapore 139951*
Indonesia: *Cyber 2 Tower, 6 F. Unit D2, Jalan H.R. Rasuna Said KAV. X5 No.13 Kuningan Timur, Setia Budi, Jakarta Selatan, D.K.I. Jakarta Raya 12950, Indonesia*

Data Portability and Data Innovation Provisions

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

Xfers comment: We agree that data portability can provide users, businesses and the economy many opportunities to properly harness the currency of the data age. However, in order to do so, the data portability and data innovation provisions must aim to mitigate the challenges associated with data portability by setting detailed industry-specific guidelines on the various operational challenges posed by data portability. These are the grounds upon which we lay most of our feedback and proposals in this consultation paper response.

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

a) scope of organisations covered; and

Xfers comment: NIL

b) scope of data covered?

Xfers comment: We agree on the coverage of the "User Provided Data" definition set forth in Paragraph 2.25 of the Data Portability Consultation paper. However, with regards to "User Activity Data" in Paragraph 2.26, we request that PDPC kindly provide a few clarifications on this matter. We will examine this from our perspective in the Payment Services Industry, hence we will primarily focus on transaction data as the main form of User Activity Data being ported and ask questions pertaining to specific examples.

1. **Third Parties' Personal Data which were NOT provided by the requesting user (c.f. Paragraph 2.30):** In a user's transaction history on a payment platform, the personal data of the counterparty to the transaction is also part of the transaction information. A transaction involving User A transferring funds to User B would record both parties' information, such as their name/contact/transacted amount. This is in contrast with PDPC's example in Paragraph 2.30 where requesting user providing personal information of his/her travelling companions because in our case, User B's data was collected by us as part of the sign-up process and not provided by User A. Stemming from this, we have a few questions based on the following example:

   Example
   Users A and B possess e-wallets on Platform A. When User A initiates a transaction with User B on Platform A, User A will see User B's personal information in their transaction details, for example User B's identity or contact information.

a. Firstly, this transaction was carried out by both parties. The personal data of both parties is included in the transaction data. When User A requests their data be ported to another organisation, will User B's consent be required to port User A's transaction data which includes User B's personal data?

   In other words, is the third party information (User B's personal data) to this transaction classified as "generated by the user's activities", or does it fall outside of this classification? If it is outside the scope of this classification, would consent then be required of the third party to disclose their information to another organisation in a data porting exercise?

b. If the personal identifying information of parties to transactions with User A is embedded in the transaction data as above, what is the minimum amount of User B's data that must be ported to meet the Data Portability Obligation? Alternatively, should such third party data instead be completely anonymised?

2. **Data Portability and Confidentiality Agreements**: Further, in the case of third parties' personal data which was NOT provided by the requesting user, can confidentiality agreements (with the third parties) be valid grounds for withholding the portation of specific confidential (but not "commercial confidential information" as PDPC has defined it) data to other organisations?

   Example
   Xfers has merchants / freelancers using our platform for payment processing. Merchant/Freelancer ABC has a confidentiality agreement with Xfers. User A who transacts with Merchant/Freelancer ABC on Xfers' payments platform requests their data to be ported to another organisation. However, confidential information (pricing, product information, identifying information, the nature of Merchant/Freelancer ABC's relationship with Xfers) is naturally embedded as part of the transaction data in User A's transaction history.

   a. Will this Data Portability Obligation have the force of law under the PDPA such that, in general, we will be able to disclose such information under general exemptions in confidentiality agreements (noting that most confidentiality agreements allow for disclosure of information if "required by law")?
   b. If information pertaining to the Merchant/Freelancer ABC is anonymised during the data porting exercise, will this fulfill our Data Portability Obligation?

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

Xfers comment: We agree with the concept to protect the incentive for first movers' business innovation. However, we request that PDPC provide organisations illustrations of situations in which they may invoke this exception relating to commercial confidential information, as well as to what extent data must be ported if part of the dataset being ported contains commercially confidential information.

b) the proposed exception for "derived data"?

Xfers comment: We agree with the exception to the Data Portability Obligation for "derived data".

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

Xfers comment: We have 2 further proposals regarding the handling of data portability requests.

1. Proposal to increase data porting timeframe from 7 calendar days to 30 calendar days instead; and
2. Proposal to make the Data Portability Obligation conditional upon technical feasibility

1. Proposal to increase data porting timeframe from 7 calendar days to 30 calendar days instead

Under Paragraph 2.37(d)(ii), PDPC has suggested that the prescribed time-frame of data porting be no more than 7 calendar days.

We propose that:

1. Instead of the current 7 calendar day time-frame for porting data, we instead adopt a 30 calendar day time-frame as is in-line with other jurisdictions as well as to have allowances for operational difficulties in execution of porting.
2. Furthermore, where appropriate justifications are given to users and PDPC, we also propose allowing time extensions to carry out data porting.

Proposal 1: Explanation

While we understand that data portability exists to ensure consumers retain the rights to their data as far as possible, we urge PDPC to increase the time-frame of porting to 30 days in consideration of the following:

1. **Other Jurisdictions:** Looking at other jurisdictions' approach, we can see that this 30-day timeframe is reasonable.

GDPR Comparison: Under GDPR article 12(3)[1], the data controller shall provide information upon request to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of requests.
CCPA Comparison: Under the California Consumer Privacy Act (CCPA) s.1798.130(a)(2)[2] a business shall disclose and deliver the required information within 45 days of receiving a verifiable request from the consumer. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary.

2. **Practical Issues:** It may not be practical to set a time-frame as short as 7 calendar days on the porting of data as an organisation may have to overcome multiple challenges in retrieving that data and formatting it in the required interoperable structure.
    a. **Technical Complications:** For example, if a financial business has stored the transaction data of a long-time user in their legacy database as well as their current database, the extraction of that user's data would take additional time and effort due to this irregularity. This is simply one of many possible technical complications that could arise, and one that is relatively common among organisations.
    b. **Large Data Volume:** The volume of a user's data may be very large and could be intermingled with other confidential commercial data, making organising and sieving relevant data more resource intensive.
    c. **Data Formatting:** Different receiving organisations could have different agreements for data porting or requirements with respect to the data being ported, necessitating the porting organisation to factor in such variability into their data porting processes, protracting the data porting process.

    When multiple such exacerbatory factors come into play, it may become difficult to entertain all data portability requests within the time-frame prescribed. Furthermore, when considering that many data porting requests could be made simultaneously, it is evident that it is not feasible to expect organisations to fulfill such requests rapidly while also carrying out core functions.

Proposal 1: Conclusion

With time, as organisations view data portability as a regular operational activity, employ established systems to carry it out or are more able to automate it, expected data porting times can be cut down and regulations can then begin to reflect this.

[1] **GDPR, art.12(3) -** https://eur-lex.europa.eu/eli/reg/2016/679/oj#d1e2172-1-1
[2] **CCPA, s.1798.130(a)(2) -** https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Considering that data portability is a relatively new concept however, allowing organisations sufficient time to adapt and overcome the hurdles in the way of achieving data portability would require the time-frame to be significantly longer than 7 days as is evident from the time-period allotted in other jurisdictions. This is why we believe that it is reasonable to have a 30-day time-frame (with extensions made permissible for valid reasons) for the porting of data.

2. Proposal to Allow Flexibility in Mode of Data Porting

We believe a reasonable approach should be taken in the adoption of technical compatibility with other organisations, which is why we believe that when it is technically infeasible to port data to another organisation, inconvenience to users should be minimised while organisations should have sufficient flexibility to meet their Data Portability Obligation.

In such situations, we propose that organisations be obligated to provide users their personal data in the relevant machine-readable format, such that they can transfer their data to another organisation by themselves.

Proposal 2: Explanation

As the Data Portability Obligation proposed would require porting organisations to directly transmit the data to receiving organisations, there may arise situations where the porting and receiving organisations experience friction in areas such as encryption standards, formatting of data, system architectures, to name a few.

> **GDPR Comparison:** The inclusion of such this proposal would be similar to GDPR Recital 68[3] and would function only to clarify the obligations of organisations and cover all the bases. This GDPR recital clarifies the obligation of organisations to directly port from organisation to organisation where this is technically feasible. This is included without damaging the overall emphasis on organisations' obligations to maintain technical compatibility and to port data directly amongst one another.
>
> **CCPA Comparison:** Looking at the CCPA s.1798.100(d)[4], requested data is provided to consumers to then be ported to other organisations by the users themselves. This directly contests with the spirit of PDPC's Data Portability Obligation and the GDPR which direct organisations to carry out inter-organisation data transfers.
>
> In contrast to California's approach, the proposal we suggest is but a minor addition to cover the rare situations where there is incompatibility in porting data between organisations. This does not take away from the overarching emphasis

[3] **GDPR Recital 68 -** http://www.privacy-regulation.eu/en/recital-68-GDPR.htm

[4] **CCPA s.1798.100(d) -** https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375

on organisation to organisation data porting which would better meet user needs and generate more innovation in the economy.

Proposal 2: Conclusion

In general, there would rarely exist barriers to data porting that render it technically infeasible. Further, PDPC will continue to prescribe the responsibilities of organisations to maintain technical compatibility with each other through regulations, notices as well as other means such as the Data Sharing Framework released by the IMDA on 28th June. This will ensure the thrust of the Data Portability Obligations remains true to the intentions of PDPC even with our proposed tweak.

As time passes, situations where technical infeasibility arises would grow ever-rarer, hence the inclusion of such a clause would only protect organisations from short-term growing pains, easing the long-term transition to a fully data portable economy.

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?

Xfers comment: We agree that PDPC should have power to review organisations' actions with respect to data portability. We have two proposals that PDPC can take into consideration.

1. Proposal for flexibility in charging fees
2. Proposal for cure period prior to imposition of penalty

1. Proposal for Flexibility in Charging Fees

As PDPC reserves the right to review and reduce the fees charged if deemed not reasonable, we propose that PDPC view an increase in porting fees to be reasonable under certain circumstances, such as but not limited to cases where individual users make repeat data porting requests.

Proposal 1: Explanation

For users who make excessive requests and abuse the data porting functionality, organisations should have a means to increase, proportionally, porting fees to deter such behaviour. This could be detrimental to the organisation as the time and resources it takes to carry out data porting can be significant and are variable subject to many factors.

To reduce the chances that an organisation has to shift significant resources away from its core functions to facilitate excessive data porting requests, the ability to impose fair but proportionally higher fees on repeated data porting requests is a simple allowance to nip this problem in the bud.

CCPA Comparison: Our proposal is similar to the condition stated in CCPA s.1798.100(d)[5] whereby users can only request such access to their data up to twice a

[5] **CCPA s.1798.100(d) -** https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375

year. While California limits outright the number of data porting requests per year, we only suggest that flexibility in imposing fees be given to organisations so that a more calibrated approach can be taken. This will best serve both organisations and users.

2. Proposal for Remedy Period prior to Imposition of Penalty

We propose that the response to failures in meeting porting requests should be measured, and as a result, we are of the view that after PDPC review, organisations should be guaranteed a minimum amount of time to remedy their failure to port data or to moderate their fees, and so on.

If organisations fail to meet such requests within that time frame (or an extended time frame given valid reasoning or extenuating circumstances), the relevant penalties and private damages may then be sought out from those organisations.

Proposal 2: Explanation

Currently, referencing Paragraph 2.47 of the Data Portability Consultation Paper, breaches of Data Portability Obligations would be subject to the same penalty framework as a breach of the Data Protection Provisions under the PDPA, exposing organisations to the risk of serious penalties subject to breaches of the provisions of the PDPA. We believe that the response to reasonable delays in meeting such requests should be measured as the act of porting data can be complex and subject to many potential hindrances.

CCPA Comparison: Our proposal is similar to CCPA s.1798.150(b)(1)[6] which provides for a period of time to cure violations of the CCPA, allowing organisations 30 days to rectify their failures to meet their Data Portability Obligations. This approach preserves users' rights to data portability while allowing organisations to meet users' requests within a practical time-frame.

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?

Xfers comment: We welcome the implementation of subsidiary legislation to create common standards for data porting as we foresee that the operational aspect of data porting will be a challenge since each organisation currently stores data very differently. However, balancing this against allowing organisations to freely make decisions pertaining to their operational efficiency requires the common standards to be general and open to changing as technology develops.

We have a few suggestions as to how this balance can be achieved with respect to Paragraph 2.49 of the Public Consultation Paper on Data Portability:

1. **Consumer Safeguards**

[6] **CCPA s.1798.150(b)(1) -** https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375

With reference to the cooling-off and pre-port verification/viewing[7] measures which were put forth, we have a few clarifications to make.

Under Paragraph 2.37(c), PDPC mentioned that users should be able to remove data that they do not wish to be ported. However, the extent of selectivity granted to users should be appropriately defined. While we wish to retain the rights of users to their data as far as possible, we also believe the practical aspect of organisational operations should be taken into consideration.

Proposal

We propose that users have control over disclosure of the 'classes' or 'columns' of information[8]**.** Rather than allowing users to control each individual transaction, users should be able to select or deselect certain columns of information from being ported.

For example, a requesting individual may see the following:

TrxnID	Date	Payee	Amt	Description	….
0001	1/1/2011	Best Toys Pte Ltd	S$ 127.22	2 x NERF guns 6 x NERF balls *[provided by Payee when charging the user]*	
0002	1/1/2011	Rachel Tan	S$ 20.00	Split dinner bill at Fish & Co *[typed in by user when sending money to friend Rachel]*	
0003	3/1/2011	Lucy Design Studios	S$ 55.00	Custom logo design work	
…	…	…	…	…	

We suggest that it is more practicable to allow requesting individuals to choose which "columns" to export rather than giving them the option of ticking "row-by-row.

Explanation

This is to maintain operational practicality, as there could be hundreds of thousands of individual data points, making it not only difficult for organisations to allow users such granular control over each 'row/cell in the table', but incredibly inconvenient for users to go through line-by-line.

[7] opportunity to view the data before it is transmitted

[8] for example, in the context of transaction information, classes of information could refer to the sender or receiver information/transacted amount/goods or services information/date/third party information/further information relating to each party to the transaction

User control over the data to be ported needs to be tempered by practicality, hence any subsidiary legislation suggested by PDPC should take this into account.

2. **Counterparty Assurance**

We agree that there should be clear criteria for the verification of receiving/porting organisation identity to guard against potential fraud. Setting regulations to guide the processes by which verification takes place will reduce friction considerably, and we support this fully.

3. **Interoperability**

We agree that to achieve the maximum benefit to the industry and to consumers, there must be sectoral codes of practice which better facilitate the transfer and usability of information across businesses. To improve the approach taken by PDPC in this undertaking, we offer a few suggestions:

a. **Set requirements for data formats rather than listing exhaustive, whitelisted formats:** While we do want to prevent fragmentation, technology develops rapidly hence we should prevent creating inertia in the industry which could cause consumers to lose out on improvements in software/technology. For example, JSON is the current accepted format for the organisation of data, but there are potential novel alternative formats such as 'Protocol Buffers', to name one, which could turn out to be more practical or effective than JSON in certain applications. So long as new formats continue to meet the general requirements set, they should not be excluded.

b. **Standardise the structuring/ordering of individual pieces of data:** For example, if Business A formats names as "First Name, Last Name" while Business B formats them as "Full Name", or if Business A only records the digits of NRIC in certain columns while Business B records the full NRIC, these arbitrary differences could create significant friction in data transfers which could be easily and painlessly avoided by setting industry protocols in the ordering of common personal data and user activity data.

4. **Security of Data**

We agree that the security of data in transit is of utmost import, not only because it is a possible target for malicious actors, but also because it is an area of potential friction between organisations when security standards differ and data cannot be transferred between them. Hence, we are in full support of PDPC's clarification of the security standards required of different sectors.

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 purposes?

Xfers comment: We support PDPC's innovation/market-oriented approach in allowing organisations to use personal data for the specified business innovation purposes without the requirement to notify and seek consent to use personal data for those purposes.

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

Xfers comment: We are generally supportive of the definition of derived data as its scope is wide enough to cover the various purposes a business could have for processing raw personal data. This allows us to continue enriching our users' experience without concern of losing confidentiality of commercial/business-specific information.

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

Xfers comment: We agree with this proposal as it allows businesses more freedom to create business innovation techniques/methodology with the personal data of users, without compromising significantly users' right to port their data where they see fit.

- END -