RESPONSE TO PUBLIC CONSULTATION

Consultation Topic:	Public Consultation on Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions
Organisation:	Tokio Marine Life Insurance Singapore (TMLS)

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

TMLS is, in principle, supportive of PDPC's proposed data portability obligation. In the longer term, it will provide consumers many potential benefits and support Singapore's Smart Nation efforts, as well as facilitate the move towards a Digital Economy.

As alluded to in the consultation paper, there will be a compliance cost impact for organizations, especially to the small and medium-sized enterprises. Many of the larger organizations may have more resources to implement the required changes, as they have already implemented, or are progressively doing so, a more customer-centric view of their data. Smaller and older firms may face greater operational challenges to consolidate customer data, even in electronic form, as the data may be fragmented across several databases and systems. In other words, how matured a company is in its data management and digital transformation journey will determine how well it is able to meet the data portability obligation.

An unintended consequence of applying the data portability requirement across the board may be the widening of an already unlevel playing field, as smaller and older firms may have inherent structural disadvantages. Newer firms may not face similar challenges as they tend not to have legacy systems and their systems are likely to have been designed in a customer-centric approach from the start.

Given the structural changes needed, in the short to medium term, the market and economy may only reap some of the benefits of data portability. It would be constrained to some extent if the broad-based transformations do not occur first. For a more sustainable digital economy in future, a more holistic approach is required to enable more companies to level-up and increase the network effect that data portability can bring about.

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

a) scope of organisations covered; and

b) scope of data covered?

a) The scope of the organizations covered is almost all the companies in Singapore. More clarity should be provided to avoid operational ambiguity on "having a presence in Singapore". For example, does it refer to representative offices, non-profit organizations, businesses exempted under the Business Names Registration Act, entities in coworking space, etc? Such entities may be representing overseas entities and have just a minor footprint in Singapore, not listed in ACRA, etc, which may circumvent the intended purpose of restricting to just Singapore entities.

   For ease of implementation, it may be useful to have a single source (e.g. registered under ACRA or another government body) where entities can check if the data portability obligation is applicable to them.

   It may also be difficult to verify the requesting individual's identity and know the situations where a person may validly act on behalf of an individual. An area that may be a little grey is on "deemed to have been given", as it may be open to interpretation.

b) Some of the data held by companies include scanned documents (e.g. PDFs or TIFF files), where certain fields may not be currently captured in databases. For example, a policyholder's source of income, which is assessed for affordability and money-laundering aspects, may be a certified copy of a bank statement, payslip, etc, that is subsequently scanned (and may not be easily machine readable). Would the scope of data covered include such scenarios? Clarity should thus be provided to avoid ambiguity, as it may be impractical to retrieve all scanned records and digitalize them into machine-readable format.

   Also, would insurance premium paid be considered as "user activity data", as technically, most of the time it is fixed and not typically generated by the use of the "product or service". Also, some insurance policies have wellness programs (e.g. steps tracker) tied to them. If this is considered "user activity data", the amount of data may be voluminous and there may need to limit the extent of data to be ported over. In addition, chatbot conversations with customers may voluminous too, and it may not be practical to include it in the data scope.

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"?

a) The exception is a useful safeguard against anti-competitive behaviour. However, it may not be sufficient on its own, as it may be difficult to independently assess if certain data are indeed "commercially confidential". What recourse is there if a monopoly or large company refuses to share its data on "commercial confidential" grounds, and what protection is there if an existing group of companies "bully" a new entrant to the market by making an excessive number of requests for data to be ported over? There may thus need to be a fair and equitable dispute resolution mechanism to handle such cases, either administered by PDPC itself or an independent party. There may be other practical problems to operationalize this exception, such as having clear guidelines on what are deemed "commercial confidential", the penalties to prevent undesirable behaviour and incentives to foster the appropriate data sharing culture.

b) The exception for "derived data" is a good start to differentiate it from user provided data and user activity data. The examples listed are good illustrations, but given the pace of innovation, the line between "derived data" and "user activity data" may be blurred over time. For example, an app may suggest the nearest or cheapest clinic for a customer to go to as part of a panel of clinics tied to the employee benefits of the customer's company. Over a period of time, this "derived data" may be discernible from the "user activity data" of the customer, based on the pattern of claims. The exception may thus be made less effective if there is no limit to the amount of "user activity data" that can be ported over. The underlying issue is thus to what extent is a company obliged to provide under the "user activity data". Certain limits, either time-based (e.g. last 1 year), volume-based (e.g. last 20 transactions) should be agreed upon by respective industries or communities.

   On "business contact information", TMLS is of the view that it should not be included under the proposed data portability obligation. Firstly, it is a deviation from the current practice of excluding it, and may thus cause some confusion and inconsistencies, and secondly, it may be subjected to abuse. For example, an agent migrating from one financial advisory firm to another may use this to move information pertaining to his customer-base and transactions (which may fall under "user activity data") over to the other firm. As such, is the intent on "business contact information" to be restricted to just "user provided data" in this scenario? As the intent of the data portability obligation is to facilitate greater control over personal data, and not business-related data, the request by the individual should be confined to solely personal matters and not commingle with business activities.

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

The operational flow described in the consultation paper is fine in general. It may need to have some flexibility, as some steps may not be practical under certain circumstance. For example, the "verifying the data to be ported" may not be feasible if the data is voluminous. It may also not be economically feasible to preserve the requested data for a long period of time too (e.g. more than 2-3 months), so a reasonable timeframe should be provided as a guide for companies.

Regarding the "withdrawal of request", it may not be appropriate to allow the requester to withdraw the request (at no cost) any time before the data is transmitted. This is because some cost will be involved throughout the period and if the request is withdrawn at the eleventh hour, it would not be fair to the company. This is because the operational work had been carried out and there may be further costs involved to cease the transmission of data. There should be a standard timeframe (e.g. 3 working days) whereby withdrawals after that will need to be charged a fee, and companies should have the discretion to charge additional fees to prevent spurious requests.

For clarity, data portability requests should not be applicable to Group Insurance or Corporate Solutions data, i.e. employee benefits and insurance data. That is, employees should not on their own accord, be able to make such data portability requests on insurers, as it impacts the employee's company as a whole.

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?

The intent of the proposed powers is good in theory, but there are numerous practical challenges. Firstly, PDPC may not understand the idiosyncrasies of every industry, the value of the data in the industry's context and the operational difficulties of the companies involved, to be an effective ombudsman. PDPC may thus need to rely on independent subject matter experts and respective authorities to assist, to prescribe the required guidelines. Secondly, it will need a framework to work with relevant regulators to ensure that the appropriate remediation measures are carried out in accordance to industry and regulatory practices. Thirdly, PDPC may face challenges in determining reasonable fee levels in various industries, in order to adjudicate on fee disputes.

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?

The codes of practices may be difficult to legislate as practices may vary from industry to industry and there is no apparent precedence in turning these

practices into legally binding requirements. If this is to be carried out, they must be thoughtfully implemented and have some flexibility incorporated into them. This is because companies in each industry may be at different operational maturity levels and the burden may fall more heavily on smaller firms. Support and time should be provided to help companies make the necessary transitions before legislating the codes of practices.

It may be useful to consider trialling the proposed data portability obligation with some clusters or sectors first, and iron out the operational issues before a broader rollout to all organizations. The lessons learnt in such a trial may benefit other clusters or sectors in future.

More time should be given for PDPC to engage the relevant sector regulators and industry stakeholders to weigh the advantages and disadvantages of the proposed approach. For example, the codes of practice may need to be non-binding at first, and a suitable timeframe be determined before legislating them.

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?

The proposed approach is laudable and a step in the right direction. Safeguards should be put in place to mitigate unscrupulous companies abusing personal data under such caveats, such as mandatory disclosure requirements, penalties and annual PDPC enforcement reports to highlight negative trends and remind industries on the appropriate governance, risk and compliance practices for a safer and effective market.

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

For clarity, the definition of "derived data" should include metadata, i.e. data that describes other data, especially if metadata is not considered as processed data. Some metadata may not necessarily be created through processing of other data by applying business-specific logic or rules, e.g. file size of uploaded claims, userid of person submitting a claim through an app (i.e. it may be someone doing it on behalf of another), etc. Such metadata may be used for business innovation purposes and should be exempted as well.

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

The indicated obligations are clearly not relevant for derived personal data. The Accuracy and Retention Limitation Obligations should also not be applied to derived personal data, as such data may be probabilistic in nature (e.g. using

artificial intelligence algorithms) and embedded in neural networks as part of the machine learning processes.

Conclusion

The proposed data portability obligation and data innovation provisions will have long term benefits and are good and necessary enhancements to the PDPA. There will be some short to medium term challenges, and these can be overcome via extensive consultations with all relevant stakeholders. Such enhancements are significant in nature and they should not be rushed into implementation. Support and incentives should also be provided to small and medium-sized enterprises to enable them to first transform themselves for the digital economy, and secondly to then contribute to the eco-system and enable Singapore to reap fully the benefits sought by the proposed changes.