PUBLIC CONSULTATION ON
THE DRAFT PERSONAL DATA PROTECTION (AMENDMENT) BILL

SUBMISSION BY THE STARHUB GROUP

28 May 2020

Contact : Tim Goodchild
Address : StarHub Ltd
67 Ubi Avenue 1
#05-01 StarHub Green
Singapore 408942
Phone : 6825 5061
Email : timothy@starhub.com

1. INTRODUCTION:

StarHub Ltd (**"StarHub"**) welcomes the opportunity to provide feedback on the Public Consultation on the Draft Personal Data Protection (Amendment) Bill ("**Bill**").

StarHub is pleased to provide its comments to the Bill as follows.

2. STARHUB'S COMMENTS ON THE CONSULTATION:

PART II: STRENGTHENING ACCOUNTABILITY

(a) Accountability principle

StarHub welcomes the explicit reference to accountability and agrees that it will make it clearer that organisations are accountable for personal data in their possession or under their control, and in relation to which they are expected to be able to demonstrate compliance.

(b) Mandatory data breach notification requirement

(i) StarHub welcomes the prescription of the numerical threshold and the categories of personal data which, if compromised in a data breach, will be considered likely to result in significant harm to the individuals. This helps to clarify the types of data breaches that require organisations to notify affected individuals.

In addition, StarHub also welcomes prescription of a notification period, as it provides clarity for organisations on when they must notify the Commission. However, rather than three calendar days, StarHub respectfully suggests that the cap be changed to three business days, as organisations are likely to require external assistance with identifying details of the breach from third party professionals, and such external assistance might not be readily available outside of normal office hours.

(ii) In relation to the proposed 'whitelist' categories, although StarHub agrees that these would provide clarity to organisations in determining what would constitute significant harm to an individual, the categories of personal data in the 'whitelist' should be carefully considered. Certain categories of personal data may not be as sensitive as others and should not be included in the 'whitelist'.

(iii) In addition, StarHub respectfully believes that the scope of credible grounds as set out in the Bill needs to be further defined. At its current state, it is open to interpretation and might lead to confusion among organisations.

(iv) StarHub respectfully suggests that the Commission provide certainty on whether the Commission should be notified before or at the same time as the affected individuals. Otherwise, this could result in the affected individuals being notified in situations where the Commission would have otherwise directed that they should not be notified.

(v) StarHub agrees that there may be situations where affected individuals may not be required to be notified of the data breach. We believe that greater clarity on the turnaround time, from the time the organisation notifies the Commission of the data breach and the Commission directing that the affected individuals not be notified, would help organisations to better plan and act in their data breach remedial plans.

(c) Offenses relating to egregious mishandling of personal data

StarHub takes the view that the accountability of individuals who handle or have access to personal data is already covered by the employment contract and any other agreements that the employee signs with the organisation. The Commission should therefore define the circumstances under which the individual could be prosecuted for such offences, as these might lead to the following situations:

- Employees not wanting to have access to such personal data, even though their job entails having access to such personal data.
- Employees being extremely cautious with their handling of such data, leading to an increase in administrative delays.

PART III: ENABLING MEANINGFUL CONSENT

(d) Enhanced framework for collection, use and disclosure of personal data

StarHub respectfully agrees with the need to enhance the framework for the collection, use and disclosure of personal data under the PDPA to ensure meaningful consent by individuals, complemented by accountability requirements to safeguard individuals' interest. StarHub takes the view that the Commission should further provide greater clarity on when and how the expanded deemed consent and the two new exceptions to the consent requirement may be used.

In relation to the 'legitimate interests' exception, StarHub notes that the exception cannot be relied upon to send direct marketing materials to individuals. Although there is a similar exception in the GDPR, that exception does not contain this carve-out as it is recognized that marketing may be a legitimate interest. StarHub respectfully submits that this exception under the PDPA should be aligned with the GDPR.

PART IV: INCREASING CONSUMER AUTONOMY

(e) Data Portability Obligation

StarHub would like to highlight that it takes time, effort and cost to set up the systems and processes to comply with Data Portability obligations. The initial cost to set up the relevant systems would be significant, and may be irrecoverable with no forecast demand for Data Portability in sight.

StarHub respectfully believes that the requirements would need to be clearly defined, so as to facilitate the implementation of Data Portability. Allowing Data Portability without clear definitions would have the following consequences:

- Organizations will have to spend substantial amounts of time, effort and money to prepare their data so as to comply with the obligations, only to find that such requests are far and few in between and hence, such costs would ultimately not be recoverable; and
- Organizations will have to spend time defining the scope in accordance with their own interpretation, which may not be what the individuals are seeking for, and the receiving organization may not be able to readily accept the data and / or to further process it.

In addition, StarHub respectfully suggests that the Commission provide clarity on whether incremental costs in responding to the Data Portability request may be recovered from the individual making the request.

(f) Improved controls for unsolicited commercial messages

StarHub respectfully agrees that improved controls for unsolicited commercial messages would help to ensure that organisations communicate more effectively with customers who are interested to receive information on offers of products and services.

StarHub suggests that the Commission define the types of unspecified commercial messages that are sent to IM accounts, to provide clarity to organisations. In addition, we believe that many of the parties sending out such unspecified commercial messages might be based overseas. StarHub therefore respectfully seeks clarity on how the Commission intends to take action against such parties that are not incorporated in Singapore, nor have an office, place of business or assets in Singapore.

PART V: STRENGTHENING EFFECTIVENESS OF ENFORCEMENT

(g) Increased financial penalty cap

StarHub respectfully agrees that increasing the maximum financial penalty will serve as a stronger deterrent. StarHub is of the view that this limit appears to be a very big leap from the existing financial penalty of up to S$1 million for data breaches, given that the

maximum financial penalty of S$1 million was only given in the SingHealth/IHiS enforcement case[1]. StarHub takes the view that increasing the maximum financial penalty will not necessarily make organisations better stewards of the personal data that they collect and are supposed to safeguard. StarHub respectfully believes that other measures such as improvements to the organisation's processes and posture toward data protection could complement the financial penalty.

Therefore, we respectfully suggest that if the financial penalty is to be increased to 10% of an organisation's annual turnover, this should nevertheless be capped at a maximum amount of S$4 million.

PART VI: OTHERS

(h) Preservation of personal data requested pursuant to access and porting requests

(i) StarHub is of the view that the prescribed period of (a) at least 30 calendar days after rejection of the request, or (b) until the individual has exhausted his/her right to apply for a reconsideration request to the Commission or appeal to the Data Protection Appeal Committee, High Court or Court of Appeal, whichever is later, might lead to the following consequences:

- Organisations might not be aware if an individual intends to appeal or not. This would result in organisations retaining large amounts of personal data beyond the specified retention period, if the organisation were to take a pessimistic approach and keep a copy of the personal data.

- This could result in an unreasonable time frame for the organisation to adhere to, as we will have no visibility of how long the appeal process would take. In addition, this goes against the Retention Obligation, as the organisations would be forced to retain such personal data for no other purpose than to comply with a possible appeal of an access request.

(ii) This extended time frame and the lack of visibility on whether the individual intends to appeal or not, might in turn, result in disproportionate administrative and technical costs to preserve a copy of the individual's requested personal data.

(iii) StarHub respectfully suggests that a maximum prescribed period of 90 days would be a reasonable period to preserve this personal data that has been requested for.

[1] Breach of the Protection Obligation by SingHealth and IHiS, 15 Jan 2019 (https://www.pdpc.gov.sg/all-commissions-decisions/2019/01/breach-of-the-protection-obligation-by-singhealth-and-ihis)

(i) Prohibitions to providing access

While StarHub respectfully recognises the need to reduce the scope of prohibitions to access in relation to user provided and user activity data, StarHub is of the view that the Commission will need to provide clarity on the situations where access to personal data, would also allow the inclusion of third-party data.

With the example of CCTV footage provided in the document, StarHub understands that with the current prohibition to providing access, it has caused implementation issues. The changes might ease the implementation issues, but at the same time, introduce a different issue where "sensitive" third party personal data is released to the requesting individual. Examples of such "sensitive" third party personal data could include:

- Prominent members of society in a compromising situation
- Security detail of a Member of Parliament

Such a situation could result in that third party individual making a claim against the organisation for revealing their personal data without their consent. The Bill should ensure that organisations are sufficiently protected against such claims such that they should have no liability for the same.

(j) Excluding "derived personal data" from Correction and Data Portability Obligations

StarHub respectfully agrees that organisation be required to provide individuals with access to derived personal data to ensure organisations remain accountable for personal data in their possession or under their control. However, greater clarity needs to be provided on what constitutes derived personal data.

3. CONCLUSION

In conclusion, while StarHub welcomes majority of the amendments, StarHub is of the view that a number of the items require more clarity from the Commission, so as to avoid confusion in the actual implementation/execution.

StarHub is grateful for the opportunity to provide feedback on the Consultation, and we hope that the Commission will consider our comments.