Response to Public Consultation on Proposed Amendments to the PDPA

28th May 2020
Rocky Howe

1. Amendment to s21(4)

The amendment to Section 21(4) removes the requirement that for an organisation to not inform you that it has disclosed your personal data to a law enforcement agency without your consent, its disclosure must either be necessary for any investigation or proceedings, or that there must be written authorization (Schedule 4(1)f&n). There has been no justification provided for this change, with no reference to this amendment can be found in the consultation paper or previous public consultations.

In a response to queries on how the short consultation period was decided in this instance, the Data Regulation secretariat replied that the reason why the consultation period was so short is that policy positions were set out through previous consultations.

MCI and the relevant law enforcement agencies should provide clarification on the intended use, justification for the necessity of this amendment. This amendment should be subject to further public deliberation.

2. Introduction of Section 35B, 35C, 35D

While the introduction of these offences were mentioned briefly in Recommendation 4.4 the Public Sector Data Review Committee, the offences themselves were not subject to previous public consultation. There are significant concerns about the proposed offences:

- The wording of the bill is extremely broad, and vague on the matter of whether disclosing one's own personal data under the possession or control of an organisation or public agency is an offence. The amended bill should minimally make clear that disclosing one's own personal data is not an offence. This is in keeping with the many parts of the Act which state that the right to give/deny consent for data sharing resides with the individual. The clarification can be inserted in the definition of individual in 35B/C/D(3).

- Further, an offence with such wide applicability leaves unclear whether it will be applied in circumstances such as journalistic reporting, not to mention day-to-day sharing of personal data between individuals. The consultation paper sets out a few scenarios that it does not apply to, but there are many more undiscussed which conceivably fall within scope of the proposed amendment. While PDPC might set out further scenarios where it does not intend criminal sanctions to apply, amending the text itself provides more legal certainty.

- The law targets personal data that is 'in the possession or under the control'. But possession or control of personal data might not fall exclusively with any one organisation, whether private or public. The personal data, of the same content, might be held by multiple organizations at once. This creates potential confusion as to whether any one organisation authorizing disclosure or use

is sufficient to avoid sanction, or the question of whether particular kind of personal data being more common results in it being authorized, or lowering the bar for reasonably believing that its disclosure is authorized.

- The PSDRC highlighted that the introduction of these offences are meant to create accountability for 'egregious mishandling' of personal data (Annex F-4). The committee did not define 'egregious mishandling' in this instance. However, the use of authorization by the organisation as a threshold for criminality, rather than a standard of threat to safety used in different parts of the PDPA itself, sets the bar extremely low for criminal punishment. Hence the proposed offences risk being overly punitive.

As a matter of principle, 35D serves a different function compared to 35B and 3C. 35D criminalizes the de-anoymization, applicable logically in circumstances where the personal data in question would have been deemed sensitive enough to necessitate increased anonymization in the first instance. Hence 35D serves a privacy protection function.

However, 35B and 35C simply penalizes the use or disclosure of data in the possession of or under control of an organisation. This would seem to be underpinned by the idea that the right to the personal data resides with the organisation or public agency who has the ultimate power to authorize disclosure or use, rather than the individual of whom the personal data is about. It should be noted that this is contrary to the principles behind other parts of the proposed amendments, such as the data portability obligations, where individuals have more autonomy and control over their own personal data.

35B and 35C should be fundamentally reconsidered, and subject to further public deliberation. Not doing so risks diminishing an individual's right to their own personal data.

3. Proposed amendments to Schedule 2

This schedule introduces what is labelled in the consultation paper as the "business improvement exception" to the need for consent in using personal data. This, however, raises concerns in organizational settings where the use of data to improve services is largely driven by algorithms:

- In cases where behavioral data and profiling using algorithms are used, automated processing of data can lead to a risk of bias or discrimination. The Commission can consider imposing obligations on organizations to assess whether the algorithms they use risk systematic bias or discrimination. They must also be able to generate an explanation for each decision that is processed automatically.

  In the alternative, the Commission can consider as an example Art 22 of the GDPR imposes restrictions on solely automated processing of behavioral data, including profiling, in cases where there is significant legal impact on individuals, such as processing credit applications. This is unless there is explicit consent from the individual.

4. Balancing widening business ease in processing personal data with individual privacy

In expanding deemed consent, and introducing the 'legitimate interest' and 'business improvement' exceptions to the need for consent, there is a significant widening of the capacity of organizations to collect, use, and disclose personal data for their purposes.

In order to balance business ease with individual privacy interests, this widening should come with the corresponding mechanisms that confer individuals a meaningful way of engaging with organizations on their concerns about how his/her personal data is being used. Such mechanisms not only act as a safeguards for the rights of individuals to their data and privacy, it also institutionalizes opportunities for individuals to seek accountability from organizations. However, these are lacking in the proposed changes.

It is recommended that the Commission consider implementing:

- A procedure for objection to the use of personal data, similar to Article 21 ('right to object' of the GDPR, where individuals can raise concerns as to whether organizations are using their personal data in line with their PDPA obligations, or if data is not used in accordance with the individual's reasonable expectations.

- Transparency requirements, in the case of the 'business improvement exemption' from consent, for organisations to make available information about how it is using the personal data of individuals.

- Further extending the retention limitation obligations in the PDPA to be aligned with Art 17 of the GDPR ('right to be forgotten'), where individuals may interface with an organisation to request the deletion of data, and where withdrawal of consent may lead to an obligation to immediately delete personal data.

- Write into legislation a legal right for individuals to interface with organisations to correct inaccurate personal data or complete incomplete data, just as in Art 16 of GDPR ('right to rectification').