May 28, 2020

Ministry of Communications and Information of Singapore

Personal Data Protection Commission of Singapore

Re: Public Consultation for the PDP (Amendment) Bill

Contact person: Chris Perera
Chris.perera@intl.att.com
AT&T Worldwide Telecommunications Services Singapore Pte Ltd
85, Science Park Drive, Singapore 118259

Summary of Major Points

Singapore is a leader in the area of data protection, and AT&T welcomes the efforts of the MCI/PDPC to add flexibility to the Personal Data Protection Act of 2012 (PDPA) and to modernize it. We offer comments on the four key areas in which amendments have been proposed, as well as some additional observations.

Statement of Interest

AT&T Worldwide Telecommunications Services Singapore Pte Ltd (AT&T) is a Facilities Based Operations (FBO) Licensee, providing enterprise services to multinational companies operating in Singapore.

AT&T has a resolute commitment to the privacy and security of our customers and users. Our global privacy program is based on four basic principles that explain our commitments to Transparency, Security, Choice and Control, and Integrity. These principles are reflected in the AT&T Code of Business Conduct, as well as our Privacy Policies. AT&T's Chief Privacy Officer is responsible for overseeing and enforcing the company's privacy principles, policies and commitments across all affiliated companies.[1]

Comments

Singapore is a leader in the area of data protection, and AT&T welcomes the efforts of the MCI/PDPC to add flexibility to the PDPA and to modernize it. We respectfully offer comments on the four key areas in which amendments have been proposed, as well as two additional observations:

- We propose that notification of a personal data breach to the PDPC be required "without undue delay following the determination that a breach has occurred";

[1] See https://about.att.com/csr/home/privacy.html.

- We welcome the expansion of exceptions to explicit consent for collection and use of personal data but suggest that direct marketing be included, subject to the individual's opt-out choice;
- We welcome the MCI/PDPC's thoughtful approach to data portability and offer considerations regarding the data that should be subject to portability;
- We offer that the increased penalties proposed appear excessive;
- In terms of additional observations, we submit that the definition of "personal data" could be amended to conform to international standards, and that section 26 might clearly incorporate additional grounds for the cross-border transfer of personal data.

Strengthening accountability

AT&T supports the desire of the MCI/PDPC to amend provisions of the PDPA that would provide for stronger organizational accountability. Requirements that an organization demonstrate privacy by design and conduct privacy risk assessments are consistent with the OECD Privacy Framework and international best practice.[2] Organizations such as the Information Accountability Foundation have published recommendations for data protection authorities and policymakers regarding how accountability principles may be put into practice.[3]

The MCI/PDPC should consider whether updates to sections 11 and 12 of the PDPA might include accountability elements such as the aforementioned. For example, section 12 might require that organizations conduct impact assessments for uses of sensitive personal data or when the use of personal data presents a risk of harm to individuals. Such an assessment represents a better use of an organization's resources than a requirement to perform assessments for processing

[2] *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79 ("OECD Privacy Framework") Part III, para. 15.
[3] See, e.g., A Path to Trustworthy People Beneficial Data Activities, Information Accountability Foundation (March 2020).

of non-sensitive personal data which takes place in the everyday course of business as a substitute for obtaining the individual's consent. Additionally, the existence of a documented privacy program and the implementation of accountability measures should be a mitigating factor in any enforcement action against an organization.

AT&T supports the proposal to require organizations to notify the PDPC and individuals in the event of a breach of personal data in circumstances in which significant harm is likely to result or where a large number of individuals are impacted. Such a requirement is also consistent with international data protection principles and best practice. The proposal to define through regulations specific categories of personal data which are likely to result in harm to individuals when breached is also constructive and will be helpful to organizations.

With regards to timeframe for notification, we respectfully submit that amendments to the PDPA should reflect the flexible standard of notice "without undue delay following the determination that a breach has occurred." The investigation and information-gathering that a business must undertake in the event of a breach in order to assess the type of data that has been accessed and the risk of harm to individuals is complex, and it may require considerable time and resources. Short notification requirements may lead to a misappropriation of resources that are better devoted to thoroughly investigating a suspected breach and remedying it to prevent further harm. It can also be counterproductive to provide hasty notice to authorities and individuals, particularly if a business determines that no breach has occurred and must then notify these parties a second time. Although the European Union's General Data Protection Regulation (GDPR) requires notice to authorities within the proposed period, there are indications that this has overwhelmed some supervisory authorities without providing a commensurate benefit.[4]

[4] Angelique Carson, Dispatch from Paris: DPAs are flooded with complaints, IAPP Privacy Advisor, February 19, 2019, available at: https://iapp.org/news/a/dispatch-from-paris-dpas-are-inundated-flooded-with-complaints/;

Enabling meaningful consent

International standards for the protection of personal data establish that individuals should receive timely notice regarding the collection of their personal data and be able to exercise choice and control over its collection, use, and disclosure.[5] At the same time, data protection principles are inherently flexible, aimed at restricting potentially harmful uses of data while allowing for many beneficial uses. As currently drafted, the PDPA is somewhat rigid in enumerating specific exceptions to the consent requirement, but at the same time, attempts to provide flexibility in sections 15 and 18 create ambiguity.

AT&T welcomes the MCI/PDPC's proposal to expand the exceptions to individual consent in sections 15 and the new section 15A, which add flexibility and clarity to the PDPA. The proposed exceptions to express consent for contractual necessity and where notification is provided strike the right balance between allowing use of personal data in the ordinary course of business and providing individuals with control. Similarly, the added flexibility provided by proposed amendments to the First and Second Schedules regarding legitimate interests and the improvement and development of goods or services are also welcome. We would suggest that the MCI/PDPC consider whether impact assessments should be required for ordinary uses of non-sensitive personal data, or whether, alternatively, the existence of a privacy program and notice to individuals may be sufficient safeguards for such uses.

Mathew J. Schwartz, Data Breach Reports in Europe under GDPR Exceed 59,000, GovInfoSecurity, February 19, 2019, available at: https://www.govinfosecurity.com/data-breach-reports-in-europe-under-gdpr-exceed-59000-a-12006.

[5] The principles of Collection Limitation, Purpose Specification, and Use Limitation are contained in the OECD Privacy Framework, and they reflect the principles stated in the Madrid Resolution (2009) of the International Conference of Data Protection and Privacy Commissioners. See also, APEC Privacy Framework, Collection Limitation, Uses of Personal Information, Choice.

We would add that use of personal data for marketing and advertising an organization's services presents a low risk to the rights of individuals and allows organizations to expand and to thrive in a competitive economy. Such uses of data are permitted by the EU General Data Protection Regulation (GDPR) and the Federal Trade Commission's (FTC) framework for privacy in the United States, and individuals may opt out.[6] AT&T would ask the MCI/PDPC to consider whether the proposed exceptions to consent in the amended PDPA could incorporate a similar approach.

Increasing consumer autonomy

AT&T commends the MCI/PDPC's deliberate approach to including the fairly novel concept of data portability in amendments to section 26. While the private and public sectors can derive great benefits from the liberation of personal data, data portability mandates may present challenges for individual privacy, data security, and the proprietary information of organizations.

For these reasons, we would propose that amendments to section 26 place further limitations on the personal data that is subject to portability. The PDPA should limit porting to personal data provided to an organization, excluding "user activity data." Such a limit relieves the burden on organizations of retaining data in personally identifiable form in order to respond to porting requests. As the PDPC develops regulations to implement the portability requirement, it should allow ample opportunity for stakeholder input.

Strengthening the effectiveness of enforcement

---

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation"), OJ L 119, 4.5.2016, p. 1-88, recital 47, Article 21(2); U.S. Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, 40-41 (March 2012) ("FTC Privacy Framework"), available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

AT&T recognizes the desire of the MCI/PDPC to provide robust protections for personal data through the amendments to the PDPA. Nevertheless, we respectfully submit that the criminal penalties contained in the new Part VIIIA appear to be disproportionate. Additionally, the broad definition of "harm," which includes "harassment, alarm or distress caused to the individual" creates a subjective standard for imposing these significant penalties. We would ask the MCI/PDPC to consider whether administrative fines might strike a better balance of the interests at stake. Furthermore, increasing the financial penalty cap to ten percent of an organization's annual gross turnover in Singapore is an extremely punitive measure, which does not appear commensurate with violations of a personal data protection law.

Additional observations

AT&T wishes to make two additional observations while the MCI/PDPC is in the process of amending the PDPA. First, the MCI/PDPC should consider amending the definition of personal data to that which is commonly found in international data protection standards. The OECD Privacy Framework defines personal data as "any information relating to an identified or identifiable individual"; the APEC Privacy Framework uses a nearly identical definition.[7]

Second, an amendment to section 26 regarding the transfer of personal data outside Singapore could recognize more flexible bases for transfer, such as those contained in the APEC Cross-Border Privacy Rules system, of which Singapore is a member.

As the MCI/PDPC are aware, the cross-border transfer of data is essential to the global digital economy, and governments should ensure that these transfer mechanisms are predictable and interoperable. Governments can build trust in the global economy – and specifically in the cloud computing and IoT industries – by creating an environment for service providers to follow

[7] OECD Privacy Framework, Part I, para. 1(b); APEC Privacy Framework, Part II, para. 9.

industry best practices and guidelines regarding the cross-border use and protection of personal data, while providing appropriate accountability mechanisms for those who wish to challenge data management practices. Agreements such as the APEC Cross-Border Privacy Rules Framework and the EU-US Privacy Shield are positive examples of such mechanisms. Organizations should also be able to rely on standard contractual clauses that are interoperable with other regional data protection regimes.

We welcome the leadership that the Government of Singapore has demonstrated at ASEAN in order to promote personal data protection and cross-border data flows. The MCI/PDPC can continue to set an example for the region by codifying flexible but robust mechanisms for the transfer of personal data in an amended PDPA.

Conclusion

Thank you for the opportunity to provide input to the MCI/PDPC consultation on amendments to the PDPA. We would be pleased to lend support to your offices throughout the process of strengthening Singapore's data protection regime.