AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com

Ministry of Communications and Information / Personal Data Protection Commission

By email to: **DataRegulation@mci.gov.sg**

May 2020

Dear sir,

Public Consultation for the Draft Personal Data Protection (Amendment) Bill

Kaspersky welcomes the amendments proposed for the Personal Data Protection Act (PDPA) and supports the Ministry of Communications and Information in its objective to enhance accountability in personal data protection through a risk-based approach and additional steps to build consumer confidence in the use, management and protection of their personal data given the advent of technological development and increasingly innovative and competitive technology products and services.

We are grateful for the opportunity to provide feedback (comprising a summary of our key points, statements of interest, and comments in response to specific aspects of the proposed amendments), as appended in the successive pages of this document.

For more information, or to discuss the contents of this submission, please contact our Head of Public Affairs, APAC, Ms. Genie Gan at genie.gan@kaspersky.com.

Thank you.

About Kaspersky
Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters to them most. Learn more at www.kaspersky.com.

AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com

Kaspersky's feedback on the Draft Personal Data Protection (Amendment) Bill

We preface our submission by highlighting (as listed below) what we view to be positive steps toward a more robust data protection framework in Singapore:

1. Enhanced institutional framework for greater cybersecurity and cyber-maturity as a result of explicit inclusion of the accountability principle into the PDPA and the introduction of a mandatory data breach notification;

   The explicit incorporation of the accountability principle creates a security-based mindset and flags to organizations the critical importance of proper personal data protection, which enables trust and confidence in modern data management practices.

   The mandatory data breach notification regime would result in greater security for individuals, as well as encourage organizations to protect themselves better through well-planned incident response and remediation policies to avoid significant reputational and financial losses. Additionally, mandatory obligations would help collect evidence-based data on which industries, sectors and organizations require additional support in personal data protection, as well as reveal any 'blind spots' in the existing framework that resulted in a failure to prevent a breach and, therefore, requires improvement.

   The additional benefit of a data breach notification would be that an individual's awareness of cyber hygiene and precautionary measures for personal data protection (such as changing passwords more often, greater attention to personal data storage and sharing with third parties) will be heightened.

   We also consider the proposed thresholds for a timeline (three calendar days) and reach in case of significant risk to affected individuals (data breaches affecting 500 or more individuals) to be appropriate, reasonable and aligned with existing data protection regulatory frameworks, without increasing compliance burden for organizations. The exceptions proposed (remedial action and technological protection) for a data breach notification would also help avoid reporting of minor and non-critical incidents, and therefore would ensure efficiency in implementation and oversight by the Commission.

   Additionally, we welcome the requirement in the Amendments to carry out a risk assessment before notifying about data breaches, and at the same time call for amending the guide to data protection impact assessment given the mandatory nature of the data breach notification regime. In the context of the Global Data Protection Regulation (GDPR)[1], many controllers notify of alleged breaches without first having conducted a risk assessment for fear of incurring hefty fines. The very broad scope (of 'unlikely to result in a risk') in the GDPR leads to many trivial notifications, placing a heavy burden on regulators, resulting in their failing to identify truly relevant cases and in a timely manner.

[1] https://iapp.org/news/a/ico-warns-about-over-reporting-data-breaches-under-gdpr/

Notwithstanding the above, we would recommend a more consistent approach to specifying the types of data that are relevant for purposes of provisions on data breaches. More specifically:

a. The public consultation documents highlight that 'data breach refers to any unauthorized access, collection, use, disclosure, copying, modification, disposal of personal data, or loss of any storage medium or device on which personal data is **stored**'.
b. We see a lack of attention in the definition to data 'in transit' and data 'in use' – widely accepted notions in the industry along with data 'in rest' (meaning being stored). From that, we see a risk of creating legal loopholes when a data breach occurs while the data is being transmitted or actively used/processed.
c. We therefore recommend amending the definition as follows: 'data breach refers to any unauthorized access, collection, use, disclosure, copying, modification, disposal of personal data, or loss of any storage medium or device on which personal data is stored**, used and transmitted**".

2. Greater consistency in personal data protection due to enhanced accountability of third-parties handling Government data;

   The proposed amendment provides strong personal data protection and ensures a consistent approach in the case of non-Government entities acting on behalf of public agencies. The existing exception in the PDPA for these organizations creates loopholes and may pose significant risks to individuals and affect their confidence in the data management and protection processes authorized by public agencies, particularly out of fear of abuse.

3. Reasonable cybersecurity and research-related derogations for re-identification;

   The proposed amendments provide reasonable derogations for the use of re-identification in the case of a cybersecurity research and investigations as well as research-related activities. These derogations would provide legal security to researchers who conduct legitimate research to uncover inadequate anonymization as a flaw in the technical design to ensure personal data protection.

4. Greater efficiency in the use and processing of personal data resulting from additional lawful grounds for personal data processing and data portability.

   The introduction of new exceptions to consent and thus inclusion of an additional legal basis for personal data processing provide greater opportunities for the use of personal data that is lawful and, at the same time, innovative and beneficial for individuals themselves.

   The legitimate interest exception that is intended to 'detect or prevent illegal activities or threats to physical safety and security, ensuring IT and network security; and prevent misuse of services', would provide cybersecurity vendors with sufficient functionality to provide data security to individuals.

In addition, further consideration of particular aspects, as set out below, would strengthen the proposed framework:

A. In the context of a personal data breach, consistent definitions of what constitute data 'in transit' and 'in use' along with the data 'in rest' to be protected (please see para 1(a)-(c) above);

B. Clear organizational and technical measures to enable secure and safe data portability;

The proposal to introduce portability presents an important milestone in the personal data protection legal framework, and empowers individuals to have greater control over their personal data in data-driven economies. Free portability of personal data from one organization to another can be a strong mechanism in fostering digital services and interoperability of platforms.

- However, the security and privacy risks correspondingly increase when systems are more interconnected given the potentially voluminous data being processed, such as when the integrity and confidentiality of data are compromised arising from careless porting of personal data.

- We therefore recommend the development of clear guidelines on the format and rules for personal data porting with the use of appropriate organizational and technical security measures. Auditing and archiving of access and back-up mechanisms are common security measures for ensuring interoperable systems with personal data processing. Accordingly, the access and exchange of personal data should be secure and implemented with access control strategies and polices, secure communication channels and high standards to prevent any unauthorized access.

- However, it should be clearly specified that, in case of porting personal data that includes information about third parties, the organization needs to consider whether transmitting that data would adversely affect the rights and freedoms of those third parties. Where practicable, reasonable steps should be taken for informed consent to be sought from relevant third parties. The onus of proving the 'reasonableness' of steps taken remains with the organization. However, this burden of proof should not be an onerous one that would result in the organization having to expend excessive resources in taking these steps which would not commensurate with the gravity of potential consequences arising from the lack of reasonable steps taken.

- The liability of organizations in the case of data portability should also be clarified. If an organization provides personal data directly to an individual or another organization in response to a data portability request, there has to be clarity as to who is responsible for further processing of that data. Individuals should also be kept informed of these liability aspects. For comparison, the GDPR has also faced criticism for not specifying any obligation, under the right to data portability, to check and verify the quality of the data which an organization transmits, though there is an obligation to ensure the accuracy of the data.

AO Kaspersky Lab
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

+7 495 797 87 00
www.kaspersky.com
www.securelist.com

C. Clear guidelines on achieving data protection by design and by default for not only organizations processing personal data and data intermediaries, but also for producers of hardware and software for personal data use.

   Organizations processing personal data generally do not develop hardware and software themselves but rely on readily available hardware and software operating systems and applications. For greater security and data protection by design and by default, we recommend developing clear guidelines in terms of practical organizational and technical measures for both organizations and producers.

   For reference, there are known examples[2] of such guidelines that were produced by the competent authorities of another data protection legal framework and were shared in the public domain. We at Kaspersky once took part[3] and provided our thoughts on enhancing a personal data protection framework through security measures.

Collectively, these proposed considerations could be further developed and clarified in a consultation with cybersecurity experts, industry and privacy advocates. We at Kaspersky would be happy to contribute with technical expertise in these consultative efforts and share further suggestions.

Thank you.

[2] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en
[3] https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/kasperskys_submission_on_the_guidelines_on_article_25_data_protection_by_design_and_by_default.pdf