BSA Comments on Draft Partial Amendment of Guidelines for the Act on the Protection of Personal Information

June 18, 2021

BSA | The Software Alliance (**BSA**)[1] appreciates the opportunity to submit the following comments to the Personal Information Protection Commission (**PPC)** regarding the draft partial amendment of Guidelines **(Draft Guidelines)** for the Amended Act on the Protection of Personal Information **(APPI)**, which was promulgated in June 2020.

General Comments

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members are enterprise software companies that create the business-to-business technology products and services that power other companies. BSA members offer tools including cloud storage services, customer relationship management software, human resource management programs, identity management services and collaboration software. Businesses entrust some of their most sensitive information — including personal data — with BSA members. Our companies work hard to keep that trust, and as a result, privacy and security protections are fundamental parts of BSA members' operations, and their business models do not depend on monetizing users' data.

Globally, BSA advocates for the implementation of national personal data protection laws that increase the transparency of personal data collection and use; enable and respect informed choices by providing governance over that collection and use; provide consumers with control over their personal data; provide robust security; and promote the use of data for legitimate business purposes.[2] BSA previously submitted comments on the Draft Partial Amendment of Commission Rules for the Act on the Protection of Personal Information[3] and appreciates the PPC providing further explanation in the Draft Guidelines on how amended APPI will be implemented. We would like to provide the below observations and suggestions to support in further improving the Draft Guidelines to provide clarity to all involved stakeholders.

[1] BSA's members include: Adobe, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, and Zoom.

[2] See BSA's Global Privacy Best Practices at: https://www.bsa.org/files/policy-filings/A4_2018_BSA_Global_Privacy_Best_Practices.pdf

[3] https://www.bsa.org/files/policy-filings/en01252021cmtsappirules.pdf

Our comments on the Draft Guidelines focus on three issues:
(1) obligations for personal information handling businesses operators with respect to reporting "leakage" of personal information, also commonly referred to as "personal data breach"[4]
(2) provisions relating to transferring data to entities in a third country
(3) the right of individuals to request cessation of use of their personal information

Observations and Recommendations

General Rules Volume / 3. Obligation of Personal Information Handling Business Operator / 3-5 Reporting etc. of Leakage etc. of Personal Data

We commend PPC for its efforts to minimize the risks of security incidents, mitigate the impact of such incidents when they occur, and reduce the complexity of compliance with security incident notification to increase their effectiveness.

In particular, BSA appreciates PPC further providing clarification on the requirements for reporting and notifying "leakage, etc." We support PPC's intention to provide transparency and enhance the rights of individuals. However, the Draft Guidelines could be improved by adjusting them as recommended below to enable business operators to focus their attention on truly meaningful incident reports and notifications.

As we noted in our earlier submission,[5] requiring reporting and notification of "potential leakage" that may not have actually occurred would raise concerns for all stakeholders involved. Mandatory reporting of "potential" leakage would not only be burdensome for organizations (as investigating and responding to incidents are both time and resource intensive) but would also result in a flood of reporting to the PPC and may overwhelm data subjects with information that hinders their ability to distinguish between inconsequential data security incidents and leakage that can cause material harm and for which they should take appropriate remedial actions.

To reduce these concerns, we recommend modifying descriptions in the following sections in the Draft Guidelines:

3-5-1-1 Concept of "Leakage"

The Draft Guidelines explain that "if all of the personal data is recovered before it is viewed by a third party, it will not fall as leakage." However, it is not clear what "all is recovered" means. In many cases, personal data may become unintentionally viewable by others due to a user's system setting error but does not result in actual data leakage. We therefore recommend supplementing this section by recognizing that data is 'recovered' when it has become accessible to others due to improper system settings by users, but there is no objective trace of unauthorized access to such data and consequently there is little risk of harm to the data subject.

3-5-3-1 Situations subject to reporting / (4) A Situation in Which the Number of Principals Pertaining to the Personal Data in Which Leakage etc. Has Occurred or Has Likely Occurred Exceeds 1,000 (*2) (*3)

The Draft Guidelines list examples of cases in which reportable leakage has likely occurred. Similar to the above, the Draft Guidelines could be improved by stating that a case in

[4] General Data Protection Regulation (GDPR) Article 4 (12): https://gdpr-info.eu/art-4-gdpr/
[5] https://www.bsa.org/files/policy-filings/en01252021cmtsappirules.pdf

which leakage etc. has “likely” occurred will be considered “a case in which there is a reasonably high degree of certainty based on the facts known at the time and on the judgement of the personal information handling business operator based on its past experience, expertise, and security measures taken etc.”. As mentioned above, in order to make reporting and notification meaningful for all involved stakeholders, we recommend clearly describing in the Draft Guidelines that even with cases shown in (*3) (a) to (d), if business operators judge that the probability of leakage etc. that results in the unauthorized access of utilizable personal information that may put data subjects at a material risk of harm is low or none, it should be excluded from being subject to reporting.

3-5-3-5 Exemption by Notification to Entruster

We also recommend the Draft Guidelines expressly recognize that in certain circumstances notification may occur outside the standard 3-5 days considered a “prompt” notification. For example, in some cases where an entrustee has entrusted to a subcontractor (sub-entrustee) and a data leakage occurs in a sub-entrustee’s system, the entrustee may require additional time to confirm the appropriate information for reporting the leakage. We recommend that the Draft Guidelines acknowledge that in such cases, it may be appropriate to extend the standard 3-5 days.

Provision to a Third Party in a Foreign Country Volume/ 5. Provision of Information at the Time of Obtaining Consent / 5-2 Information to be Provided / (2) 2) Information on the System Relating to the Protection of Personal Information in the Said Foreign Country

The ability to transfer personal data internationally is crucial to companies of all sizes and in all industry sectors. The Draft Guidelines reflect a requirement imposed by the APPI amendments that companies provide certain information to data subjects regarding international data transfers.

The Draft Guidelines also list examples of the information to be provided to a data subject regarding the system for personal information protection in the foreign country in which the third-party recipient is located. We are concerned, however, that this approach will result in different information being provided individually from different companies and could lead to confusion by a data subject that would ultimately interfere with the utilization of personal information. We therefore recommend that the information on the personal information protection system in foreign countries be based on information that PPC provides on the PPC website.

The Draft Guidelines also specify a range of information to be provided, including under (d), regarding the “existence of other systems that may have significant impact on the rights and interests of the principal.” We provide comments (below) on the two examples provided in the Draft Guidelines that purport to illustrate systems that might have such an impact.

Example 1 references “a system that allows the government to collect a wide range of information on personal information held by businesses operators by imposing on businesses operators an obligation to cooperate extensively with government information collection activities.” However, this example introduces several uncertainties, as it is not clear what will be categorized as “wide range of information” and “government information collection activities”.

Example 2 indicates “a system pertaining to the obligation to preserve personal information within the country which may not enable business operators to respond to a request for deletion, etc. from a principal.. However, how an “obligation to preserve within the country” relates to “the possibility of not being able to respond to deletion request” is not clear in the Draft Guidelines.

In implementing the Draft Guidelines in relation to “other systems that may have a significant impact”, we recommend the PPC to focus on circumstances where a business operator is unable to comply with a data subject’s demand for deletion, such as by describing: “a case in which the country’s laws prohibit a company from responding to or executing a deletion demand.”

General Rules Volume / 3. Obligation of Personal Information Handling Business Operator / 3-8 / 3-8-5 Utilization Cease etc. of Retained Personal Data / 3-8-5-1 Requirement for utilization cease / (3) 3) A Case in Which the Rights and Legitimate Interest of the Said Principal May be Harmed

One of the examples given by the PPC in respect of cases where “there is a possibility to harm the rights or legitimate interests of the principal” is the case in which a principal, who has received direct mails, requests the personal information business operator to stop sending such direct mails and the business operator does not comply.

We recommend that the Draft Guidelines explicitly state that the appropriate party to receive and comply with such stop requests (and to whom principals should send the stop requests) is the business operator responsible for initiating the mail and not a third-party intermediary or mail service that is only responsible for transmitting the mail. This is because the third-party intermediary or mail service would be acting under the instructions of the business operator responsible for initiating the mail.

Conclusion

BSA appreciates the opportunity to comment on the Draft Guidelines. We hope that our recommendation will be useful as you continue to refine the Draft Guidelines and to develop Q&A to provide further clarity on the new requirements. We appreciate the PPC taking steps to update and involve stakeholders during the development of the Guidelines and look forward to continuing conversation in the future on the topic. Please let us know if you have any questions or would like to discuss comments in more details.