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

January 25, 2021

BSA | The Software Alliance (**BSA**)[1] appreciates the opportunity to submit the following comments to the Personal Information Protection Committee (**PPC)** regarding the draft partial amendment of Commission Rules **(Draft Commission Rules)** 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's members are among the world's most innovative companies, creating software solutions that spark the economy. BSA member companies have made significant investments in Japan and we are proud that many Japanese organizations and consumers continue to rely on our members' products and services to support Japan's economy.

BSA members are enterprise solutions providers that create the software-enabled products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, cybersecurity solutions, and collaboration software. These enterprise software companies are in the business of providing privacy protective solutions and their business models do not depend on monetizing users' data. BSA members recognize that companies must earn consumers' trust and act responsibly with their personal data.

We appreciate the PPC's commitment to lead international discussions on the protection and utilization of personal data and encourage the PPC to continue promoting the harmonization and interoperability of international personal information protection systems through appropriate international frameworks.

BSA member companies have a deep and long-standing commitment to protecting personal data across technologies and business models as they recognize that technology users are only comfortable taking advantage of the benefits of new technologies if they trust that they will keep control over their personal data. BSA previously submitted comments on the Outline of Amendment of the Act on Protection of Personal Information Based on the So-called Three-Year Review in January 2020 (**Previous Submission**),[2] which we highlight here. BSA has been closely monitoring the considered direction for the implementation of the amended APPI and appreciates the PPC providing opportunities to discuss the relevant issues with impacted stakeholders.

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

[2] https://www.bsa.org/files/policy-filings/en01142020amendappicmts.pdf

BSA advocates globally 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[3]. BSA also advocates for the international interoperability of national personal data protection regimes. This is an essential component of the digital economy and should enable and encourage international transfers of personal data. Where differences exist among varying privacy regimes, BSA encourages governments to create tools to bridge those gaps in ways that both protect privacy and facilitate the free flow of data.[4]

In addition to the above, we provide specific observations and suggestions below regarding the PPC's proposed Draft Commission Rules.

Observations and Recommendations

Data Breach Reporting/Notification - Commission Rules Article 6-2, 6-3, 6-5

BSA welcomes the PPC taking into consideration BSA's previous recommendation to exclude encrypted data from the scope of the requirements regarding data breach, limiting reporting/notification requirements to those cases in which there is material risk of harm. We also support the approach of not setting a specific time limit to submit a preliminary report and allowing reasonable time for submitting definitive report. This approach will enable the performance of risk assessment by the affected business operator to determine the scope of the security risk, to initiate response measures, and to develop measures to prevent a recurrence of the incident. We also appreciate PPC's proposal to not require notification to concerned individual to be made at the same time as the reporting to PPC.

We would nonetheless appreciate it if the PPC could clarify, in the Draft Commission Rules, that if the preliminary report made to the PPC already contains all the information in items (i) through (ix) of Article 6-3(1), this would also constitute the definitive report required under Article 6-3(2), and an additional definitive report need not be submitted.

We also remain concerned about the requirement included in the Draft Commission Rules to report and notify "potential" personal data breaches have "likely" occurred. While we agree action must be taken as soon as practicable after a data breach is identified, such reports and notifications should be limited to personal data breaches that have occurred and involve the actual unauthorized acquisition of unencrypted or unredacted personal data thus creating a material risk of harm to the data subjects, such as identity theft or financial fraud. This approach requires security incidents be analyzed to determine if they should be classified as data breaches and ensures that industry's and the PPC's limited resources are used judiciously to address consequential harm from such incidents. Requiring reporting and notification of "potential breaches" that may not have actually occurred would not only be burdensome for organizations (as responding to incidents are both time and resource intensive) but would also, result in a flood of reporting to the PPC, and overwhelm the data subjects with information that they may not be able to distinguish between inconsequential data security incidents (such as unauthorized access to encrypted data for example) and breaches that can cause material harm and for which they should take appropriate remedial actions. Therefore, we urge the proposed requirement to report "potential" data incidents be removed from the Draft Commission Rules as it does not materially add to the protection of individuals against personal data breaches.

[3] See BSA's Global Privacy Best Practices at: https://www.bsa.org/files/policy-filings/A4_2018_BSA_Global_Privacy_Best_Practices.pdf
[4] BSA Privacy Framework, https://www.bsa.org/policy-filings/bsa-privacy-framework

We are also concerned about the requirement (in Article 6-3 (1) (v) of the Draft Commission Rules) to report "*whether or not there had been secondary damage or there is a possibility of secondary damage and its details*". Often, especially with respect to business operators who process data on behalf of other enterprises, there is no ability to gauge whether or not there has been any secondary damage. However, it would also not be appropriate for business operators to guess that there might be NO secondary damage and report accordingly, as there may be unforeseen or unknown circumstances that could result in secondary damage. Further, there is a possibility that even in the case where there is a possibility of secondary damage, the **probability** of the secondary damage occurring could be minimal. Given that the same information will need to be provided to data subjects, this could generate unnecessary concern among individuals, diverting their attention from meaningful notifications and resulting in inaction in both cases. To address these concerns, we recommend that Article 6-3 (1) (v) should be amended to require reporting only "*where there **had** been secondary damage or there is a **reasonable risk** of secondary damage and its details*".

Also, for a case in which notification to the concerned individual is difficult, for example, because the business operator does not have the contact information for the individuals affected by the breach, we continue to request the PPC to consider alternative mechanisms for notification. Notification to the PPC, rather than directly to individuals, may be appropriate in certain circumstances.

Cross-Border Data Transfer / Commission Rules Article 11-3

It is our understanding that a business operator must provide the following information to an individual in cases where the data transfer requires obtaining the individual's consent: 1) the name of the country to which the data will be transferred to; 2) information on the legal framework applicable to protect personal information in the foreign country to which the information will be transferred; and 3) the measures taken by the third-party recipient to protect personal information.

These requirements may not achieve the PPC's goals of increasing an individual's understanding of how his or her personal information will be handled as highlighted in our Previous Submission. The effectiveness of data security and personal information protection has little to do with where data is physically stored or processed. Instead, data security and personal information protection depend on the quality of the technologies, systems, and procedures put in place by the business operator handling the personal information, and any third-party receiving the data, including the provision of robust security measures. The business operator should remain accountable over all personal data transferred, whether domestically or internationally. For example, even though a third-party recipient of personal information is headquartered in a country outside of the EU, it may have chosen to apply the EU's data protection laws - which Japan has recognized as adequate - to all data it processes, regardless of where the data has come from or where the data is stored or processed. As such, it matters less where the personal information is stored and processed, or even where a third-party processor is headquartered, than the policies and procedures the processor adopts and implements to protect the data. Therefore, we urge the PPC to guide individuals to understand the importance of how companies, including overseas companies, protect personal information to avoid the misconception that higher security risks are associated with third-party recipients located in foreign countries compared to domestic handling of personal information.

However, given PPC's decision to impose this requirement on cross-border data transfer, we respectfully request that the definition of "foreign country" for the purpose of Article 11-3 be clarified to refer to the country in which the third-party receiving the data is headquartered. This is based on previous discussions with PPC, where we understand that, for the purposes of these Draft Commission Rules, "foreign country" is the country in which the third-party

receiving the data is headquartered, and not the country in which data centers used to physically store or process data are located. We therefore recommend the Draft Commission Rules clearly define “foreign country” in this way to avoid confusion.

Cross-Border Data Transfer / Commission Rules Article 11-4

Based on Article 24 (3) of the amended APPI, for the cross-border transfer of personal data based on the establishment of a system conforming to standards prescribed by rules of the PPC, Article 11-4 of the Draft Commission Rules stipulates that business operators should periodically confirm that the overseas third-party recipient continues to take measures equivalent to those taken by the business operators in Japan and the data protection system in the “foreign country” does not unduly impede the implementation of such data protection measures. This will ensure that the transferred personal information continues to be protected by equivalent measures by a third- party in a foreign country.

It is our understanding based on discussions with the PPC that this requirement must be satisfied once a year. We support the PPC taking into consideration this reasonable approach and would further recommend that the Draft Commission Rules confirm this point in the upcoming Guidelines concerning the Act on the Protection of Personal Information (“**Guidelines”**). We also recommend the upcoming Guidelines clearly specify what type of reporting will be considered appropriate for compliance with this requirement.

Pseudonymously Processed Information / Commission Rules Article 18-7

The standards prescribed in Article 18-7 are useful for determining how to produce pseudonymous information. It is our understanding that the PPC will present examples in the Guidelines to which business operators can refer. We ask that the Guidelines make clear that the “examples” are illustrative and that business operators may continue to adopt alternative methods of pseudonymizing personal data as long as such data can no longer be attributed to a specific data subject without the use of additional information.

Conclusion

BSA appreciates the opportunity to comment on the draft Commission Rules. We hope that our recommendation will be useful as you continue to refine the Rules and prepare Guidelines to provide further clarity on the new requirements. We appreciate PPC taking steps to update and involve multi-stakeholders during the development of implementation rules 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.

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office