BSA Comments on the Interim Summary of Issues Examined under So-called Three-Year Review of Act on Protection of Personal Information

May 27, 2019

BSA | Software Alliance (**BSA**)[1] submits the following opinions to the Personal Information Protection Committee (**PPC**) regarding the Interim Summary of Issues Examined under the So-called Three-Year Review of the Act on Protection of Personal Information (**Interim Summary**).

General Comments

BSA members lead the world in offering cutting-edge technologies and services, including cloud computing, data analytics, machine learning, and artificial intelligence. For companies to operate globally in a modern data society, it is critical that national personal information protection laws and systems be globally interoperable and that smooth cross-border data transfers are facilitated.

BSA members recognize that robust measures to protect personal information is key to building and maintaining customer trust, which is necessary if consumers and societies are to benefit from the economic and social development that modern software-enabled technologies will underpin. It is for this reason that BSA supports data protection frameworks that are user-centric, enabling consumers to control their personal information and to ensure that the use of personal data consistent with consumers' expectations while also enabling companies to pursue legitimate business interests.

To encourage these and other outcomes in the development of data protection frameworks around the world, BSA developed **Global Privacy Best Practices.**[2] The Global Privacy Best Practices support the implementation of measures 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.

Japan's amended Act on the Protection of Personal Information (**APPI**) provides effective personal information protection while facilitating the utilization of personal information. It is internationally interoperable (as demonstrated by the recognition of "adequacy" by the European Union (**EU**)) and provides mechanisms to facilitate international data transfers.

Since its establishment as an independent central authority for personal information protection, the PPC has actively promoted globally interoperable personal information

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

[2] The BSA-Global Privacy Framework: https://www.bsa.org/~/media/Files/Policy/Data/2018_BSA_Global_Privacy_Best_Practices.pdf

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

protection systems and smooth cross-border data transfers through international efforts. As described in the Interim Summary, these efforts include participation in international fora of data protection regulators and policy makers, achieving a mutual recognition of adequacy with the **EU**, and the actively promoting the Asia Pacific Economic Cooperation (**APEC**) Cross-Border Privacy Rules (**CBPR**). BSA encourages the PPC's continued leadership in these key areas.

As the PPC undertakes the Three-Year Review of the APPI and considers areas of potential improvement to Japan's existing personal information protection system, it is important to maintain these features of the law: providing effective protection of personal information; enabling the legitimate commercial use of personal data; ensuring and promoting international interoperability; and facilitating cross-border data flows.

In the section below, we provide more specific observations or suggestions for the PPC's consideration.

Observations and Recommendations:

Section 1: Individual Rights related to Personal Information

Individuals should have control over their own data and be able to request disclosure, correction, or discontinuation of use of their personal data as appropriate. On the other hand, the scope of the request should be practical and the methods to comply with it should be flexible so as not to impose unreasonable burdens on business activities.

Data Portability

Under the Section "Demand of Disclosure", the Interim Report discusses voluntary versus mandatory mechanisms for data portability, or the ability for a customer to transfer his or her data from one platform to another. The Interim Report welcomes the voluntary efforts undertaken by the private sector in this regard, but also note that under the EU General Data Protection Regulation (**GDPR**), this is a consumer right.

We support efforts to enable consumers to access and obtain a copy of the personal data that they provide to organizations. We also agree with the PPC's view in the Interim Report that any discussions around data portability must adequately consider the needs and expectations of consumers, benefits to businesses, and the costs and burdens a mandatory data portability "right" would impose.

Software service providers, including cloud service providers, tend to facilitate data migration and portability in creative and innovative ways without regulatory intervention. This is because each company has a business interest to attract customers from their competitors and will therefore make available tools to facilitate data migration. The PPC should therefore avoid developing a prescriptive regulatory approach to addressing data portability, as such approaches may be counter-productive, and would likely lead to practical operational challenges that increase the cost of compliance and lessen the incentives for businesses in Japan to use data and technology in innovative ways.

Instead of prescribing specific mechanisms or developing domestic standards for data portability, **BSA recommends that the PPC encourage the development and adoption of voluntary, transparently developed, industry-led internationally recognized standards. Business operators should retain the flexibility to determine the appropriate means and format of providing this information to the consumer.**

If the PPC decides to incorporate a mandatory data portability requirement, it should ensure that it has appropriate limitations to ensure organizations can protect legitimate business interests and the privacy and security of other consumers. Any such measures should also

preserve the flexibility associated with voluntary portability efforts, including the means and format in which the information is maintained or delivered.

Discontinuation of Use and Deletion

Under the Section "Utilization Cease, etc.", the Interim Report notes that business operators handling personal information are only required to delete and stop using personal information if the data was acquired or has been used unlawfully. This, according to the Interim Report, has caused frustration with some consumers, even though many companies voluntarily respond to customer requests to delete or discontinue the use of personal data. Many business operators comply with voluntary standards that require responses to such requests beyond those required in Articles 19 and 30 of the amended APPI.

BSA supports ensuring that individuals have control over their personal information. Implementing consumer rights that align to internationally recognized best practices and standards, including the right to request the discontinuation of use or deletion of personal information, serves to achieve this outcome. While these rights lay a strong foundation for a robust data protection framework, it is imperative that any such rights contain appropriate limitations, including to protect the rights of other consumers, and the flexibility for business operators taking into account legitimate commercial needs.

In this regard, BSA agrees with the assessment in the Interim Summary that business operators may need to retain some personal information, especially where there is a legitimate legal or business purpose to do so and complying would be impractical or significantly interfere with normal business operations. This includes for example, retaining some personal information in order to respond to future inquiries, requests, and legal claims from a data subject pertaining to personal information processing activities, without which a business' ability to respond to such claims would be adversely impacted. Other important reasons for business operators to retain some records of personal information include to protect the legal rights of other consumers, for research purposes, to detect or prevent, fraud, ID theft, or criminal activity, to comply with legal obligations, such as data retention requirements, and to ensure security.

If the PPC were to expand scope of the requirement related to the deletion or discontinuation of use of personal information, **BSA recommends that the PPC provide adequate flexibility and provide sufficient and reasonable limitations on such requirements to ensure businesses retain the ability to legitimate commercial activities**.

Section 2: Data Breach Reporting

In the Interim Summary, the PPC proposes to amend the APPI further to impose data breach notification requirements in certain circumstances. Currently, data breach reporting is not mandatory in Japan, although the PPC provides detailed guidance to business operators for when and how to report data breaches. As described in the Interim Summary, in considering making such guidance mandatory, the PPC intends to take account current business practices in Japan and developments in international discussions.

In our experience, personal information protection frameworks are most effective when they are principle-based, outcome-focused, and not unduly prescriptive. From this viewpoint, **we recommend that business operators should be required to report personal information breaches to a regulatory authority or individuals only when the personal information breach involves unauthorized acquisition of unencrypted or unredacted personal data and it creates a material risk of harm to the individual such as identity theft or financial fraud. Reporting should not be required when the stolen personal data was encrypted or there are no risks to individuals' rights or freedom.**

Finally, because it is important to ensure individuals receive meaningful notifications in the

event of a breach, it is critical that business operators are afforded adequate time to perform a thorough risk assessment to determine the scope of the security risk and prevent further disclosures before being required to report the breach. **Therefore, the APPI should not set explicit reporting deadlines for breach notifications but instead require reporting to occur as soon as practicable after the discovery of the breach.**

Section 3: Promoting Business Operators to Protect Personal Information

Effective personal information protection laws should promote corporate responsibility in a manner that frees consumers from the burden of having to determine whether to consent to each instance of personal data collection. As noted in the Interim Report, one way to demonstrate corporate responsibility is through assessments, equivalent to the data protection impact assessments (DPIAs) mandated by GDPR. DPIA's can help business operators weigh the benefits of data processing against potential impacts of data processing on the rights and freedoms of the individuals whose data is being processed. Individuals are well-protected when identified risks have been mitigated through documented safeguards, such that the benefits of processing personal data outweigh the residual risks. Affirmative consent should not be required in instances where this balance has been achieved, as demonstrated through rigorous, documented analysis. Without the ability to apply this type of balanced approach to processing data, it will become very difficult to obtain the volume and type of data that is required to advance data-driven technology, such as artificial intelligence, in a manner that ensures privacy, as well as the effectiveness, fairness, safety and security of data processing. BSA therefore supports PPC's recognition of the importance of business operators adopting risk assessments in its Interim Report.

Section 5: Penalty

Remedies and penalties for violations of personal information protection laws should be structured to be effective and proportionate to the harm resulting from such violations. BSA therefore agrees with the Interim Summary that discussions about adjusting penalties under the amended APPI must take into consideration what is effective and proportionate in Japan's context. Because, as the Interim Report describes, most companies that are informed or warned by the PPC that their conduct may be in violation of the amended APPI correct this conduct voluntarily, **it does not seem necessary to introduce new administrative fines or increase penalties**.

Section 6: Status of Extra Territorial Application of the Law, Efforts to Harmonize with International Mechanism and Status of Cross-border Data Transfer

Extra Territorial Application of the Law

With respect to territoriality, BSA advocates for data protection frameworks that govern conduct only where: (1) residents are specifically targeted, (2) the personal data that is the object of the processing is purposefully collected from data subjects in the country at the time of collection, and (3) such collection is performed by an entity established in the country through a stable arrangement giving rise to a real and effective level of activity (see BSA Global Privacy Best Practices). Considering collectively a foreign country's sovereignty; the effectiveness of personal information protection in Japan; the risk that another country would try to impose their own laws and enforce them on Japanese companies and the potential restrictions on Japanese companies' business activities; as well as the risk that companies would be commanded to comply with different laws in two or more countries, which could create significant confusion internationally, **we recommend not expanding the extraterritorial application of the APPI beyond its current scope**.

In response to the proposals described in the Interim Report that personal information acquired in Japan should remain stored locally on servers in Japan, BSA agrees with the PPC's observation that such proposals could be at odds with the Government of Japan's

positions on digital trade in the World Trade Organization (**WTO**) and could be incompatible with Japan's commitments in the Comprehensive and Progress Trans-Pacific Partnership (**CP-TPP**). In addition, as described above, the effectiveness of personal information protection has very 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 in place by the data controller, including the data controller's accountability over data transferred to data processors.

As such, **BSA strongly opposes the introduction of data localization requirements**, and we agree that such a policy would be ineffective at achieving the policy objective of enhancing personal data protection, would be inconsistent with Japan's commitments in the WTO and CP-TPP and with Prime Minister Abe's vision of Data Free Flow with Trust (**DFFT**), and would undermine the PPC's leadership in promoting digital trade globally.

BSA encourages **the PPC to continue to promote the harmonization and interoperability of international personal information protection systems and collaboration among relevant international enforcement authorities**.

Cross-border Transfer

Ensuring smooth cross-border data transfers is a prerequisite for innovation in the digital economy era. Businesses in all sectors of the economy heavily rely on smooth cross-border data transfers.

The current system in Japan works well for companies that conduct business globally. Many companies operating in Japan, and especially BSA members, already invest significant resources into ensuring that data, including personal information, is effectively protected no matter where it is stored or processed. Thus, we strongly recommend the PPC avoid imposing any further limits on international data transfers. Holding business operators accountable for the protection of personal information regardless of to whom it is transferred or where is far more effective than limiting data transfers to particular jurisdictions. As such, we hope the PPC and the Government of Japan will continue to demonstrate leadership internationally by promoting mechanisms that facilitate global cross-border data transfers, such as the APEC CBPRs, ambitious rules in the WTO eCommerce negotiations, and in Japan's bilateral and regional trade agreements.

Conclusion

BSA appreciates the opportunity to submit our comments on the Interim Summary. We hope this will be useful in finalizing the Interim Summary. We also hope to continue exchanging our opinions and collaborating with the PPC to finalize the report. Please let us know if you have any questions or would like to discuss these comments in more detail.