BSA Comments on the Outline of Amendment of the Act on Protection of Personal Information based on the So-called Three-Year Review

January 14, 2020

BSA | The Software Alliance (**BSA**)[1] appreciates the opportunity to submit the following opinions to the Personal Information Protection Committee (**PPC**) regarding the Outline of Amendment of the Act on Protection of Personal Information based on the So-called Three-Year Review (**Outline**).

General Comments

BSA members lead the world in offering cutting-edge technologies and services, including cloud computing, data analytics, machine learning, and artificial intelligence. We recognize that robust measures to protect personal information are key to building and maintaining customer trust, which is necessary if consumers and societies are to benefit from the economic and social development that are supported by modern software-enabled technologies.

For this reason, BSA and our members strongly support data protection frameworks that ensure personal data is used consistent with consumers' expectations, while also enabling companies to pursue legitimate business interests. BSA submitted our opinion regarding the Interim Summary of Issues Examined under the So-called Three-Year Review of the Act on Protection of Personal Information in May 2019 (**Previous Submission**).[2] BSA has been closely monitoring the development of the proposed amendments to the Act on the Protection of Personal Information (**APPI**) and appreciates the opportunities to discuss the relevant issues with the PPC and other stakeholders.

During this process, BSA has encouraged the PPC, as it considers amendments to the APPI, to refer to BSA's **Global Privacy Best Practices.**[3] As reflected in that document, BSA supports 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. The APPI as currently

[1] BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, 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] 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, available at https://www.bsa.org/files/policy-filings/05272019bsacommentsthreeyearreview.pdf

[3] BSA Global Privacy Best Practices, available at 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

crafted already provides many of these features.

In addition, 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 facilitate cross-border data transfers. 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.

In the section below, we provide more specific observations and suggestions for the PPC's consideration. In general, absent specific proposed legal text or more specific descriptions of the proposed amendments, it has proven difficult to provide specific and pertinent constructive feedback on the Outline. **We urge the PPC to consult with interested stakeholders, including BSA and other representatives of the international software industry, on the specific language of proposed amendments to the APPI, the draft Cabinet Order, or other draft of relevant guidelines, before submitting such recommendations to the Diet or determining the details of rules.**

Observations and Recommendations:

Chapter 3: Specific Considerations
Section 1: Individual's Rights concerning Personal Data

Individuals should have control over their personal data. BSA supports efforts to implement consumer rights that align with internationally recognized best practices and standards. Individuals should be able to request disclosure, correction, or discontinuation of use of their personal data, as appropriate. The scope of such requests and the obligations of companies to respond to them should be practical and flexible, to avoid imposing unreasonable burdens on business activities.

Discontinuation of Use and Deletion

In Section 1.3 of Chapter 3, the Outline proposes relaxing requirements regarding requests to discontinue using personal data, requests to delete personal data, and requests to stop providing personal data to third parties.

The purpose of the proposal is to expand the scope of individual rights and to provide individuals more control over their personal data. At the same time, the proposal acknowledges the need to take into consideration the difficulties business operators may experience when responding to such requests, and states that "refusal to the demand shall be allowed on an exceptional basis." BSA supports the goal of ensuring that individuals have control over their personal data.

While these individual rights lay a strong foundation for a robust data protection framework, it is imperative that any such rights contain appropriate limitations – tailored to the type of request and risk created – to avoid unintended consequences for both businesses and consumers. Unfortunately, the Outline does not provide enough detail regarding the specific circumstances in which an individual may make such requests and under what exceptional bases a business operator may legitimately decline to comply with such requests. **In particular, we encourage the PPC to focus on the exceptional bases on which companies may decline a request.** The considerations may be different depending on whether the request is for discontinuation of use or for deletion. For example, business operators may need to retain some personal data – and decline an individual's request to delete it – where there is a legitimate legal or business purpose to do so and complying with an individual's request would be impractical or significantly interfere with normal business operations. This includes, for example, retaining some personal data in order to respond to future inquiries, requests, and legal claims from a data subject pertaining to personal data

processing activities, without which a business's ability to respond to such claims would be adversely impacted. Likewise, the PPC should recognize other important reasons that companies may have to decline an individual's request to discontinue use of personal data, including when processing the information is needed to detect or prevent fraud, ID theft, or criminal activity; to comply with legal obligations, such as data retention requirements; for purposes of research; to ensure security; or to provide a good or service requested by the individual. **We urge the PPC to duly examine and consider all relevant scenarios in establishing appropriate limitations.**

It will be important for interested stakeholders to be able to review the specific language of proposed amendments to the APPI, the draft Cabinet Order, or other draft of relevant guidelines to provide more targeted feedback to the PPC.

Disclosure

Article 28 of the APPI states that a person may request a business operator handling personal information to disclose the retained personal data that can identify the individual. Section 1.4(2) of Chapter 3 of the Outline proposes that an individual may specify the method or format in which such personal information is provided, including in an electronic format and that the business operator handling personal information is obligated to disclose the information in the manner so instructed.

We recognize that consumers should be able to obtain a copy of their personal data from business operators. **We encourage the PPC to clarify that the scope of information to be disclosed to the consumer should be limited to the information that the consumer provided to the business operator, or that was created by the consumer.**

It is also important to note that there are circumstances in which it is not possible to provide a data subject information about his/her own data without disclosing information belonging to other data subjects (for example when information is part of files or databases that cannot be modified). Similarly, providing an individual with access to data may create security risks if the company is unable to verify that individual's identity. **The PPC should consider these and related factors when establishing or clarifying the right to access one's own data.**

We also encourage the PPC to ensure business operators retain flexibility in determining the appropriate format for providing information to an individual. The most appropriate and secure method for disclosing retained personal data in an electronic format may vary depending on the volume of personal data and the size, operation, IT skill, and security considerations of the company which handles the disclosure. As a result, strictly following an individual's instructions regarding format may not necessarily be beneficial for all individuals. Therefore, the methods to comply with the disclosure obligations should be flexible and any new rules should not require information to be provided to an individual in a particular electronic format.

Section 2: Responsibilities to be Observed by Business Operators

Mandating Breach Report and Notification to Individuals

In Section 2 of Chapter 3 of the Outline, the PPC proposes to amend the APPI to mandate data breach reporting for certain situations such as a breach concerning a defined number of individuals or a breach of sensitive personal information.

The focus on data breach reporting should be on the risk created to the data subject(s) and not on arbitrary factors such as the number of individuals affected. 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, such as identity theft of financial fraud, and, to the individual when that risk is high.** Reporting should not be required when an incident involves encrypted data and the encryption keys have been kept safe or there are no risks to individuals' rights or freedom.

In this regard, the current PPC guidelines on data breach reporting, 2017 PPC Notice No. 1,[4] adopt the correct approach. The guidelines state that reporting is not required if neither the personal data nor methods of generating anonymous data from personal data is deemed to have been leaked in a substantial way. We therefore urge the PPC to maintain its current position on data breach notification.

Because it is important to ensure that notifications are meaningful 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 to prevent further disclosures before being required to report the breach. In this regard, we support the Outline's recommendation not to set explicit reporting deadlines for breach notifications. We recommend the APPI require reporting to occur (both preliminary report and definitive report updating the facts/circumstance afterwards) "as soon as practicable" after the actual breach has been confirmed by an operator.

Finally, if 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 request the PPC to consider alternative mechanisms for notification and avoid imposing an obligation to publicize the breach. For example, notification to the PPC rather than directly to individuals may be appropriate in certain circumstances and could help to avoid the security risks that may result if notification of a breach is publicized.

Section 3: Approaches to Encourage Voluntary Efforts by Business Operators

Privacy Impact Assessment

Section 3.2(2) of Chapter 3 of the Outline indicates the PPCs interest in gathering industry best practices for enhancing privacy and personal information protection, including through the use of privacy impact assessments (**PIAs**). As we explained in our Previous Submission, assessments equivalent to the data protection impact assessments (**DPIAs**) mandated by the European Union's General Data Protection Regulation (**GDPR**)[5] can help business operators weigh the benefits of data processing against the potential impacts of data processing on the rights and freedoms of the individuals whose data is being processed. Such assessments can enable business operators to tailor and target the amount and types of data that are required to advance data-driven technology, such as artificial intelligence, in a manner that ensures the individuals' privacy and the effectiveness, fairness, safety, and security of data processing. BSA therefore welcomes the PPC's commitment to gather more information about PIAs or DPIAs and promote business operators' efforts for such risk assessments. We would welcome the opportunity to support the PPC in this regard.

Section 5: Penalties

[4] https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf (Japanese only).

[5] *See* Article 35, General Data Protection Directive, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Section 5 of Chapter 3 of the Outline proposes to introduce more severe penalties on business operators, including through a substantial increase in criminal penalties. In this regard, it is important to highlight that 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. As the Outline recognizes, most companies that are informed or warned by the PPC that their conduct may be in violation of the APPI correct their conduct voluntarily. As a result, we believe the PPC's focus should be continuing to provide an appropriate period for business operators to implement measures in response to the PPC's guidance, recommendations, or orders prior to the imposition of penalties. Penalties should only be applied if business operators do not take appropriate measures in a timely manner.

When penalties are imposed, the appropriate tools may include providing monetary relief to compensate individuals for any economic harm they suffer and imposing tailored conduct-based relief to prevent future violations. In contrast, criminal penalties are not proportionate remedies for violation of data protection laws and do not have a useful role to play in enforcing data protection laws. In BSA's view, the substantive requirements of a data protection law, combined with monetary relief and conduct remedies provided through administrative or civil judicial processes, are sufficient to protect individuals' privacy interests. Although we recognize that the APPI has been adopting the criminal penalties, we would like to emphasize that they should not be imposed because criminal penalties are not proportionate remedies for violation of data protection laws. Indeed, the threat and risk of criminal liability – even if limited to specific cases – can deter experimentation with beneficial and harmless data practices.

Section 6: Extra-territorial Application of the APPI, Efforts to Harmonize International Mechanisms, and Cross-border Data Transfers

Extra-territorial Application of the APPI

Section 6 of the Outline proposes an expansion of the scope of extra-territorial application of the APPI including authorizing the PPC to administratively order foreign business operators to submit reports to the PPC. The Outline also proposes authorizing the PPC to take certain measures against foreign business operators, to conduct on-site investigations, and to make public the fact that foreign business operators might be non-compliant with obligations imposed by administrative orders.

As we indicated in the Previous Submission, 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.[6] We recommend not expanding the extraterritorial application of the APPI beyond its current scope, particularly in consideration of the effectiveness of personal information protection in Japan; a foreign country's sovereignty; the risk that another country would try to enforce its own laws on Japanese companies (which could create restrictions on Japanese companies' business activities); and the risk that companies would be commanded to comply with different laws by two or more countries, which could create significant confusion internationally. Instead, 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.

[6] 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, available at https://www.bsa.org/files/policy-filings/05272019bsacommentsthreeyearreview.pdf. See also BSA Global Privacy Best Practices, available at https://www.bsa.org/~/media/Files/Policy/Data/2018_BSA_Global_Privacy_Best_Practices.pdf.

Although BSA does not support expanding the extra-territorial application of the law for the reasons stated above, if any measures in this regard were to be considered, it is critical that due process is fully observed before foreign business operators are required to comply with any additional requirements.

BSA looks forward to providing more specific suggestions to PPC once we are able to review the language of proposed amendments to the APPI.

Strengthening Restrictions on the Provision of Personal Data to Third Parties in Foreign Countries

The Outline proposes that personal information providers to third party recipients located in foreign countries shall provide information to the individual concerning the handling of personal information by the recipients, including the name of the recipient's country, and whether the system for the protection of personal information exists in that country.

In our view, these measures are unlikely to achieve the PPC's goal of increasing an individual's understanding of how his or her personal information will be handled. The effectiveness of 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 in place by the business operator handling the personal information, including the provision of robust security and the business operator's accountability over the data transfer. For example, even though a company is headquartered in a country outside of the EU, it may have chosen to apply the EU's data protection laws to all data it processes, regardless of the location of the data or the location of its processing. Therefore, we urge the PPC to guide individuals to understand the importance of how companies protect personal information and not to inaccurately believe higher security risks are associated with third party recipients located in foreign countries compared to domestic handling of personal information.

Furthermore, the rules about provision of information to individuals should not be prescriptive and should allow enough flexibility to business operators so that transparency and accountability of business operators can be facilitated without imposing an unnecessary burden. This approach would also benefit consumers. If a business operator were required to notify individuals every time it hires a new vendor that processes data in a new country, it may result in sending an individual a countless number of communications that fail to advance her privacy interests. Requiring such extensive notices to individuals on a single topic may also deter individuals from focusing on notices that do meaningfully affect their privacy rights, thereby reducing the effectiveness of other privacy-related notifications.

In addition, ensuring smooth cross-border data transfers is a prerequisite for innovation in the digital economy era. The Government of Japan is making efforts to realize Prime Minister Abe's vision of Data Free Flow with Trust (**DFFT**), and businesses in all sectors of the economy heavily rely on smooth cross-border data transfers. 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.

Conclusion

BSA appreciates the opportunity to submit our comments on the Outline. We hope this will be useful to PPC as it continues to consider amendments to the APPI and relevant regulations. We urge the PPC to consult with interested stakeholders, including BSA and other industry representatives, on the specific language of proposed amendments to the APPI before submitting such recommendations to the Diet.

Please let us know if you have any questions or would like to discuss these comments in more detail.