April 23, 2024

BSA COMMENTS ON PERSONAL INFORMATION PROTECTION ACT GUIDELINES FOR FOREIGN BUSINESSES

Submitted Electronically to the Personal Information Protection Commission

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide comments to the Personal Information Protection Commission (**PIPC**) regarding the draft English translation of the Guidelines on Applying the Personal Information Protection Act to Foreign Business Operators (**Guidelines**).

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members create the technology products and services that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration systems. Our members have made significant investments in Korea, and we are proud that many Korean entities and consumers continue to rely on our members' products and services to do business and support Korea's economy.

BSA appreciates the PIPC's efforts to provide guidance to foreign businesses. The Guidelines elaborate on key obligations in the Personal Information Protection Act (**PIPA**), advise on how these obligations are to be met, and provide examples of how the PIPA may be applied. Our recommendations below seek to ensure that important provisions in the PIPA are explained with greater accuracy and precision.

BSA's Recommendations

Guidelines	BSA's Recommendations
<u>Chapter III Part 2 (Impact of Data Processing on Data Subjects in the Republic of Korea), Page 18</u> In some cases, foreign business operators process the personal information of the Korean Data Subjects without directly offering goods or services to them. Since these actions can have a direct and significant impact on the Korean Data Subjects, and the effects and nature of these activities are foreseeable, such foreign business operators must comply with the PIPA.	**We recommend deleting these paragraphs from the Guidelines.** The language used in this section significantly expands the scope of the PIPA and cannot be reasonably enforced. The Guidelines broadly state that even where a foreign business operator does not offer goods or services to Korean data subjects, they may have to comply with PIPA requirements if their actions have significant impact on them. To ensure that these Guidelines are effective in

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, ESTECO SpA, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

(Case 9) Foreign business operators that collect the personal information of the Korean Data Subjects (e.g., names, addresses, and phone numbers) and then share this information publicly on a website or utilize it for service provision must comply with the requirements under the PIPA, such as establishing a legal basis for the processing of personal information. This is the case even if they do not directly offer services to these Korean Data Subjects.	both implementation and enforcement, they should be limited to governing conduct that has a sufficiently close connection to Korea. Obligations should apply to businesses only if they offer goods and services to data subjects in Korea. The extension of PIPA's applicability to any foreign business in the absence of their obvious or implicit targeting may cause unnecessary challenges with compliance and enforceability and result in conflicts with other international privacy laws such as the European Union's General Data Protection Regulation. For instance, with such interpretation in place if there was a data breach or unauthorized access caused by an external actor which triggers a regulatory notification requirement under the PIPA, a foreign business operator shall be expected to notify the regulator if the compromised data includes personal data of a few Korean data subjects even where the operator's business does not offer goods and services in Korea or where the breach itself did not target Korean data subjects. Thus, this is impractical and cannot be reasonably enforced.
<u>Chapter III Part 2 (Impact of Data Processing on Data Subjects in the Republic of Korea), Page 19</u> The PIPA may also apply when a foreign business operator receives personal information of the Korean Data Subjects from a Korean business operator and processes such information for its own business purposes. (Case 12) When a foreign business operator receives and processes the personal information of the Korean Data Subjects and related artificial intelligence learning data collected by the Korean business operator to develop an artificial intelligence model, the foreign business operator must comply with the PIPA.	**We recommend deleting these paragraphs from the Guidelines.** The language and the example case used in this section would make the scope of PIPA overly broad and challenging for foreign businesses. It is not practical to apply the PIPA to foreign business operators that do not offer goods and services in Korea. With reference to Case 12, the development and training of cutting-edge technology and tools, most notably AI models, require vast datasets which may sometimes contain personal information. An example would be an AI-powered Human Resource Management tool. However, a receiving business operator, whether foreign or domestic, receiving such information likely will not be able to identify Korean Data Subjects from the datasets. In this regard, as a general principle, obligations that involve interfacing with the Korean Data Subject, e.g., notifying the Korean Data Subject, should always be placed on the Korean business operator that collects personal information directly from the Korean Data Subjects. Such obligations should not apply to the business operator, whether domestic or

	foreign, to which the Korean business operator subsequently discloses the datasets.
<u>Chapter III Part 3 (Place of Business Located within the Republic of Korea), Page 21</u> Since the PIPA defines a "data subject" as "an individual who is the subject of the processed information," it may include foreign individuals. Therefore, Korean entities that process the personal information of foreign data subjects may also be required to comply with the PIPA. However, for foreign individuals located outside Korea, the processing of their personal information might be governed by the laws of the country that regulate the data subject. Consequently, applying the PIPA in such cases could lead to jurisdictional conflicts over the same activities between multiple countries. In this scenario, if the processing of personal information does not affect domestic affairs in Korea, there may not be significant rationality or justification to apply the PIPA in addition to foreign personal information protection laws. Therefore, based on the specifics of each case, the processing of personal information of foreign individuals outside of Korea may be primarily subject to the laws of other countries. However, if the personal information of foreign data subjects being processed within Korea is infringed, necessitating action from the Korean government, or if a Korean or foreign business processes the personal information of foreign individuals located overseas in countries lacking adequate personal information protection laws, or where such laws exist but are unreasonably insufficient, necessitating protection under the PIPA, the application of the PIPA may be considered.	**We recommend deleting this paragraph:** **"*However, if the personal information of foreign data subjects being processed within Korea is infringed, necessitating action from the Korean government, ~~or if a Korean or foreign business processes the personal information of foreign individuals located overseas in countries lacking adequate personal information protection laws, or where such laws exist but are unreasonably insufficient, necessitating protection under the PIPA,~~ the application of the PIPA may be considered."*** We agree with the Guidelines that processing personal information of foreign individuals outside of Korea is subject to the personal information protection laws of their countries. As such, the PIPA would not apply. However, the paragraph above suggests that the PIPA will also apply where the personal information of foreign individuals is processed in Korea, and the countries of these foreign individuals have "unreasonably insufficient" personal information protection laws, which would "necessitat[e] protection under the PIPA". We disagree with this interpretation. Whether a country has "adequate personal information protection laws" is not relevant. In the absence of specific guidance on the personal information protection laws of each country, a business operator would not be able to determine if a foreign data subject's country has "unreasonably insufficient" personal information protection laws. This would create further uncertainty for businesses when assessing if the PIPA applies.
<u>Chapter IV Part 1 (Notification and Reporting of Divulgence of Personal Information), Pages 23-25</u> Upon discovering a divulgence of personal information, it is mandatory to inform the affected data subjects about the matters prescribed by the PIPA within 72 hours. If the divulgence involves the personal information of	**We recommend the following changes:** **"*If the divulgence involves the personal information of 1,000 individuals or more, includes sensitive or personally identifiable information, or results from unlawful external access, it must be reported to the PIPC or the Korea Internet & Security Agency ("KISA") within 72 hours. ~~The mere~~***

1,000 individuals or more, includes sensitive or personally identifiable information, or results from unlawful external access, it must be reported to the PIPC or the Korea Internet & Security Agency (**"KISA"**) within 72 hours. The mere awareness that unauthorized third parties could have gained access to the personal information is considered sufficient recognition of the divulgence. … Additionally, even if there is a possibility that unauthorized individuals could have accessed the personal information system, making the personal information potentially known to them, it may not constitute divulgence if there is definitive evidence that no unauthorized third party has actually viewed or accessed the information.	~~***awareness that unauthorized third parties could have gained access to the personal information is considered sufficient recognition of the divulgence.***~~**"** Businesses should only be required to notify personal information breaches when 1) they have actual knowledge of a successful (not a potential) breach of personal data and 2) the breached personal data presents a meaningful risk of harm to data subjects. The statement that "***mere awareness*** that unauthorized third parties ***could*** have gained access to the personal information is considered sufficient recognition of the divulgence" (emphasis added) suggests that the threshold for determining whether breach is a notifiable breach is far less than actual knowledge, based on evidence of a successful breach. Use of the term "mere awareness" implies that a preliminary assessment, short of an actual determination, is sufficient to trigger the PIPA's obligations. Furthermore, use of the word "could" implies that definitive evidence of unauthorized access is not necessary in determining if there is recognition of divulgence. These factors lead to a situation where the mere *possibility* of unauthorized access would meet the threshold for determining sufficient recognition of divulgence. We disagree with this application of the PIPA — there must be definitive evidence of an actual breach or unauthorized access before determining if there is recognition of divulgence And only actual breaches with a reasonable risk of harm to data subjects should be subject to reporting to either data subjects or the KISA. Otherwise, the requirements as written risk flooding both data subjects and KISA with notifications, reducing the ability of both to assess and take steps in response to meaningful breaches involving personal information. In addition, this statement does not recognize the exception set out in Page 25 that "even if there is a possibility that unauthorized individuals could have accessed the personal information system, making the personal information potentially known to them, it may not constitute divulgence if there is definitive evidence that no unauthorized third party has actually viewed or accessed the information".

Chapter IV Part 2 (Disclosure of the Privacy Policy) When disclosing the privacy policy on a website or the like, it is essential to label it clearly as "Privacy Policy" and use design elements like font size and color to distinguish it from other notices such as terms of use, ensuring that it is easily recognizable by data subjects. Upon revising the privacy policy, the prior versions of the privacy policy should remain accessible so that data subjects can access them at any time. It is advisable to present the changes comparatively, highlighting the before and after to make it easy for data subjects to understand what has been changed.	**We recommend the following changes:** ***"When disclosing the privacy policy on a website or the like, it is essential to label it clearly as "Privacy Policy" and ~~use design elements like font size and color to distinguish it from other notices such as terms of use, ensuring~~ ensure that it is easily recognizable by data subjects. For example, the business operator may use design elements, such as a different font size or color, to distinguish the privacy policy from other notices such as the terms of use.*** ***Upon revising the privacy policy, we encourage businesses to make the prior versions of the privacy policy ~~should remain~~ accessible so that data subjects can access them ~~at any time. It is advisable to present the changes comparatively, highlighting the before and after to make it easy for data subjects to~~ and understand what has been changed."*** We agree that the privacy policy should be easily identifiable and recognizable. However, the requirements to use different font sizes and color, and to present the "before and after" when changes are made, are overly prescriptive. In the case of presenting the "before and after", it is also not clear how many prior versions must be compared. Requiring tracking changes through multiple versions will quickly become unreasonably challenging for businesses and difficult to understand for data subjects. These should be presented as examples rather than requirements.

Conclusion

We thank PIPC for the opportunity to provide feedback on the Guidelines. Please do not hesitate to contact BSA if you have any questions regarding this submission or if we can be of further assistance.

Sincerely,

Tham Shen Hong

Tham Shen Hong

Senior Manager, Policy – APAC