2024 년 4 월 23 일

「해외사업자의 개인정보 보호법 적용 안내서」에 대한 BSA 의견서

개인정보보호위원회 귀하

BSA[1]는「해외사업자의 개인정보 보호법 적용 안내서」 (이하 '안내서')의 영문(안)과 관련하여 개인정보보호위원회 (이하 '개인정보위')에 의견을 제출할 수 있는 기회가 주어져 기쁘게 생각합니다.

BSA 는 각국 정부와 세계시장을 중심으로 글로벌 소프트웨어 산업을 대변하고 있습니다. 회원사들은 클라우드 스토리지 서비스, 고객 관리 소프트웨어, 인적 자원 관리 프로그램, ID 관리 서비스, 보안 솔루션 및 협업 소프트웨어 등 고객의 역량과 협업을 강화하는 매우 중요한 서비스들을 제공하고 있습니다. 그동안 BSA 회원사들은 한국에 상당한 규모의 투자를 진행해왔으며, 현재 다수의 국내 기업과 소비자들이 사업을 진행하고 한국 경제를 뒷받침하는 데에 있어 BSA 의 회원사들의 제품과 서비스를 지속적으로 사용하고 있다는 것을 자랑스럽게 생각합니다.

BSA 는 해외 사업자를 위한 지침을 제공해주신 개인정보위의 노력에 감사드립니다. 「해외사업자의 개인정보 보호법 적용 안내서」는 보호법의 주요 의무를 상세히 설명하고, 이러한 의무 이행 방법을 조언하며, 개인정보보호법 (이하 '보호법')을 어떻게 적용할 수 있는지에 대한 예시를 제시합니다.

다음와 같이 보호법의 주요 조항들이 보다 명확하게 설명될 수 있도록 하기 위해 제언드립니다.

[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

BSA's Recommendations

Guidelines	BSA 의견 및 추천 사항
Chapter III Part 2 (Impact of Data Processing on Data Subjects in the Republic of Korea), Page 18 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. (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.	**해당 단락의 삭제를 고려해주시길 요청드립니다.** 이 부분에서 사용된 표현은 보호법의 적용 범위를 지나치게 확대하고 있으며, 합리적으로 시행하기 어렵습니다. 안내서는 한국에서의 대상 재화 또는 서비스 제공 여부와는 별개로 해외사업자가 한국인 또는 한국 정보주체의 개인정보를 처리하여 한국 정보주체에게 직접적이고 상당한 영향을 미치고 있는 경우 보호법이 적용된다고 명시하고 있습니다. 본 안내서의 효과적인 작용하기 위해선 행위의 범주를 한국과 충분히 밀접한 관련이 있는 것으로 한정해야 합니다. 또한 사업자가 한국에서 정보주체에게 재화와 서비스를 제공하는 경우에만 의무가 적용되어야 합니다. 모든 해외 사업자에게 보호법의 적용 범위를 확대하는 것은 안내서를 준수하는데 있어서 문제를 야기하고, 유럽연합의 '일반 개인정보 보호법 (GDPR)과 같은 해외의 개인정보보호법과 충돌할 수 있습니다. 예를 들어, 외부 행위자에 의한 유출이나 권한이 없는 접근으로 인해 보호법에 따라 신고해야 합니다. 하지만 안내서는 해당 해외 사업자가 한국에서 재화나 서비스를 제공하지 않거나 유출이 한국 정보주체를 대상으로 하지 않는 경우에도, 유출된 개인정보 일부에 한국 정보주체의 개인정보가 포함되어 있는 경우 신고해야 합니다. 이는 현실적으로 이행하기 어려울 것으로 판단됩니다.
Chapter III Part 2 (Impact of Data Processing on Data Subjects in the Republic of Korea), Page 19 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	**해당 단락의 삭제를 고려해주시길 요청드립니다.** 이 부분에서 사용된 용어와 사례는 해외 사업자에게 보호법을 광범위하고 적용하여 이행을 어렵게 만들 수 있습니다. 한국에서 재화와 서비스를 제공하지 않는 해외 사업자에게 보호법을 적용하는 것은 어려움이 따를 수 있습니다. (Case 12)와 관련하여, 최첨단 기술 및 도구, 특히 인공지능 모델의 개발과 학습에는 개인정보가 포함될 수 있는 방대한 데이터

collected by the Korean business operator to develop an artificial intelligence model, the foreign business operator must comply with the PIPA.	세트가 필요할 수 있습니다. 인공지능 기반 인적자원 관리 도구가 일례입니다. 그러나 해외 사업자와 국내 사업자 상관없이 이러한 정보를 수신하는 사업자는 데이터 세트에서 한국 정보주체가 포함되어 있는지 여부를 식별할 수 없을 가능성이 높습니다. 따라서 원칙적으로 정보주체에게 이 사실을 통지하는 등 한국 정보주체와의 상호작용과 관련된 의무는 항상 한국 정보주체로부터 직접 개인정보를 수집하는 한국 사업자에게 부과되어야 합니다. 이러한 의무는 한국 사업자가 사후에 공개하는 데이터세트를 사용하는 국내, 또는 해외 사업자에게 적용되어서는 안 됩니다.
Chapter III Part 3 (Place of Business Located within the Republic of Korea), Page 21 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	**해당 단락에 대하여, 아래와 같은 내용으로 수정을 고려해주시길 요청드립니다.** **"*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.*"** 해외에 있는 외국인의 개인정보 처리시 해당 정보주체에 대하여 규율하고 있는 국가의 법률이 적용될 수 있다는 안내서의 해석에 동의합니다. 따라서 이 경우에는 개인정보보호법이 적용되지 않는 것으로 이해합니다. 그러나 위 내용은 외국인의 개인정보가 한국에서 처리되고 해당 외국인 정보주체에 적용되는 국가의 개인정보 보호법이 "지나치게 불합리"하여 "해당 정보주체를 보호해야 할 필요성이 명백한" 경우에 한국의 개인정보보호법이 적용될 것이라고 제시하고 있습니다.

PIPA, the application of the PIPA may be considered.	BSA 는 이러한 해석에 이견을 드립니다. 국가에 적절한 개인정보 보호법이 있는지 여부는 판단 기준이 되기 어렵습니다. 각 국가의 개인정보 보호법에 대한 구체적인 지침이 없는 경우, 사업자는 외국인 정보 주체의 국가에 "지나치게 불합리"한 개인정보 보호법이 있는지 여부를 판단할 수 없습니다. 이는 보호법 적용 여부를 확인할 때 더 큰 불확실성을 야기할 수 있습니다.
Chapter IV Part 1 (Notification and Reporting of Divulgence of Personal Information), Pages 23-25 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 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.	**아래 내용의 수정을 고려해주시길 요청드립니다.** **"*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 awareness that unauthorized third parties could have gained access to the personal information is considered sufficient recognition of the divulgence.~~*"** 사업자는 1) 개인정보의 유출이 발생 (잠재적 가능성이 아님) 했음을 실제로 인지하고 2) 유출된 개인정보가 정보주체에게 의미 있는 피해 위험을 초래하는 경우에만 개인정보 유출 통지의 의무가 있습니다. "유출 사실을 알게 되었을 때는 권한 없는 제 3 자가 개인정보를 알 수 있는 상태에 이르렀다는 사실을 인지하게 된 것만으로도 충족한다"는 표현은 개인정보의 유출의 발생을 실제로 인지한 경우와 비교하여, 해당 유출이 통지 대상인지 여부를 판단하는 기준이 현저히 낮다는 것을 시사합니다. "사실을 인지하게 된 것만으로도" 이라는 표현은 확정이 아닌 가능성만으로도 보호법의 의무가 적용된다는 것을 의미합니다. 또한 확정적인 증거가 유출 인식 여부를 판단하는 데 필요하지 않다는 것을 의미합니다. 이러한 요인으로 인해 무단 액세스 가능성이 있다는 것만으로도 유출에 대한 충분한 인정을 판단하는 기준이 충족되는 상황이 발생할 수 있습니다. 우리는 이러한 보호법의 적용에 동의하지 않습니다. 유출 인식

	여부를 판단하기 전에 실제 침해 또는 무단 접근에 대한 결정적인 증거가 있어야 하며, 정보주체에 대한 합리적인 피해 위험이 있는 실제 침해만 정보주체 또는 KISA 의 보고 대상이 되어야 합니다. 그렇지 않을 경우, 서면 신고 관련 내용은 정보주체와 KISA 모두에게 통지 업무가 폭주하여 개인정보와 관련된 의미 있는 침해 사고를 평가하고 대응 조치를 저하시킬 위험이 있습니다. 이와 관련하여, 25 페이지에 명시된 "권한 없는 제 3 자가 개인정보처리시스템에 접근할 수 있는 등 개인정보를 알 수 있는 상태에 있었다고 하더라도 실제 권한 없는 제 3 자에게 열람되었거나 접근되지 않은 것이 확실한 경우에는 유출에 해당하지 않을 수 있다"는 예외 역시 재고해주시길 요청드립니다.
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.	**아래와 같은 수정을 고려해주시기를 요청드립니다.** ***"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."*** "개인정보 처리방침"은 쉽게 식별하고 알아볼 수 있어야 한다는 데 동의합니다. 그러나 글자 크기, 색상 등을 활용해 변경된 사항에 대한 전·후를 비교해야 한다는 요건은 지나치게 규범적인 측면이 있습니다. '변경된 사항에 대한 전·후'를 제시하는 경우, 얼마나 많은 이전 버전을 비교해야 하는지도 명확하지

	않습니다. 여러 버전을 통해 변경 사항을 추적하도록 요구하는 것은 기업에게는 불합리하게 작용될 수 있으며, 정보주체의 이해에 방해가 되는 요소로 작용할 수 있습니다. 따라서 요구 사항이 아닌 예시로 제시하는 것을 고려해주시기 바랍니다.

Conclusion

「해외사업자의 개인정보 보호법 적용 안내서」에 대해 의견을 제공할 수 있는 기회를 주셔 감사합니다. BSA 의 제안과 관련하여 문의사항이나 의견이 있으시면 언제든지 연락 부탁드립니다.

Sincerely,

Tham Shen Hong

Senior Manager, Policy – APAC