2026 년 8 월 31 일

한국 데이터 보호 체계 검토에 관한
BUSINESS SOFTWARE ALLIANCE(BSA) 의견서

개인정보보호위원회 귀중

BSA (비즈니스 소프트웨어연합, The Business Software Alliance, 이하 "**BSA**")[1] 는 개인정보보호위원회(이하 "위원회")가 실시하는 한국의 데이터 보호 체계에 대한 종합적인 검토와 관련하여 제언을 제시할 수 있는 기회가 주어져 기쁘게 생각합니다.

BSA 는 각국 정부와 세계 시장을 중심으로 글로벌 소프트웨어 산업을 대변하고 있는 연합체로[2], BSA 회원사들은 클라우드 스토리지 서비스, 고객관계관리소프트웨어, 인적자원관리프로그램, 신원 관리 서비스, 보안 솔루션, 협업 소프트웨어 등 다양한 기업 활동을 뒷받침하는 기술 제품과 서비스를 개발·제공하고 있습니다. 또한 다수의 회원사들은 서비스형 소프트웨어(SaaS) 형태의 제품과 솔루션을 한국 경제 전반에 걸쳐 다양한 기업에 제공하고 있습니다. 이에 BSA 는, 한국 기업들이 회원사들의 솔루션을 신뢰하며, 이를 기반으로 사업을 운영하고 성장해 나가고 있다는 점을 매우 뜻깊게 생각합니다.

BSA 는 그동안 개인정보 보호 사안을 두고 위원회와 꾸준히 소통해 왔습니다. 위원회가 동의 중심의 현행 체계가 AI 시대에도 여전히 적합한지 점검하고 있다는 점을 특히 반갑게 생각하며, 현행 체계가 더 이상 제 역할을 다하기 어려울 수 있다는 위원회의 진단에도 크게 공감합니다. 오늘날 수집 시점에 받는 동의는 실질적인 보호 효과가 크지 않은 반면, 책임 있는 데이터 활용에는 상당한 제약으로 작용하는 경우가 많습니다. 개인은 쏟아지는 동의 요청 속에서 자신의 선택이 갖는 의미를 잃어가고, 기업은 사회적으로 유익하고 위험이 낮은 처리에조차 기댈 만한 법적 근거를 찾지 못합니다. 이러한 점에서 BSA 는 위원회의 재검토 결정을 환영합니다.

---

[1] BSA 회원사: Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

[2] 참고: BSA, 「개인정보보호법 시행령 개정안에 대한 의견서」, 2026 년 7 월, , https://www.bsa.org/policy-filings/korea-bsa-comments-on-draft-amendments-to-pipa-enforcement-decree; BSA, 「개인정보보호법 시행령 제정안에 대한 의견서」, 2023 년 6 월, https://www.bsa.org/policy-filings/korea-bsa-comments-on-personal-information-protection-act-draft-enforcement-decree; BSA, 「개인정보보호법 개정안에 대한 의견서」, 2021 년 11 월, , https://www.bsa.org/policy-filings/korea-bsa-submission-on-proposed-revisions-to-personal-information-protection-act.

BSA 제언 요약

제언사항 1: 정당한 이익(legitimate interest)에 따른 처리 근거 확대

- 「개인정보 보호법」(이하 "보호법") 제 15 조제 1 항제 6 호를 국제적으로 통용되는 정당한 이익(legitimate interest) 근거에 맞게 넓히고, 동의의 예외가 아니라 동의와 대등한 처리 근거로 자리매김해야 합니다.
- 해당 근거에 따른 개인정보 처리는 정보주체의 권리와 이익에 부정적인 영향을 미치지 않는 경우 허용하되, 이를 판단할 때에는 개인정보 보호상 위험을 완화하는 조치를 고려하는 이익 형량(balancing test)을 적용하고, 개인정보처리자의 이익이 정보주체의 권리와 이익보다 '명백히 우선(manifestly superior)'할 것을 요구하지 않아야 합니다.

제언사항 2: 개인정보처리 "위탁자"와 "수탁자"의 책임의 명확한 구분

- 국제 기준의 주요 개인정보 보호 법제와 정합성을 갖도록 관련 개념을 정비해야 합니다. '개인정보처리자' 중 '위탁자'는 개인정보의 처리 목적과 수단을 결정하는 주체로, '수탁자(outsourcee)'는 개인정보처리자를 대신하여 개인정보를 처리하는 주체로 정의해야 합니다.
- 각 주체의 역할에 따라 의무를 차등적으로 부과해야 합니다. 동의 획득 및 정보주체의 권리 행사 요청에 대한 대응 등 소비자와 직접 관련된 책임은 '위탁자'에게 부과하고, '수탁자'에게는 개인정보의 안전한 보호 및 위탁자의 지시에 따른 처리 등 그 역할에 상응하는 의무를 부과해야 합니다.

제언사항 3: 국경 간 데이터 이전 절차 개선

- 개인정보의 국경 간 이전이 해당 개인정보를 수집한 목적을 달성하기 위해 필요한 경우, 최초 개인정보처리에 대한 동의만으로도 해당 이전의 법적 근거를 충족할 수 있도록 '별도 동의' 요건을 조정해야 합니다.
- EU 표준계약조항(EU Standard Contractual Clauses, **SCCs**), 영국 국제 데이터 이전 협정(UK International Data Transfer Agreements), 글로벌 및 APEC 국경 간 개인정보 보호 규칙(Global and APEC Cross-Border Privacy Rules, **CBPR**), ASEAN 모델 계약조항(ASEAN Model Contractual Clauses), ISO/IEC 27701 등 국제적으로 통용되는 데이터 이전 수단을 인정해야 합니다.
- 보호법 제 28 조의 8 제 1 항 제 5 호에 따른 동등성 인정 경로(equivalence route)의 예측 가능성을 제고해야 합니다. 이를 위해 심사 기한을 명확히 규정하고, 우선순위 결정 기준을 공개하며, 우선적으로 검토할 국가에 관한 업계의 의견을 수렴하고, 해당 국가에 포괄적인 개인정보 보호법의 존재 여부만을 기준으로 판단하지 않고 해당 국가의 관련 법·제도 전반을 종합적으로 고려해야 합니다.

제언사항 1: 정당한 이익에 따른 개인정보 처리 근거 확대

현황 및 상황 **(문제 사례)**	「개인정보 보호법」은 동의를 중심에 둔 법입니다. 일반적으로 기업은 개인정보를 수집하거나 처리하기 전에 정보주체의 동의를 받아야 합니다. 그러나 실제로는 동의를 받기 어렵고 받더라도 보호 효과가 크지 않은 목적으로 개인정보를 처리해야 하는 경우가 적지 않습니다. 사기 탐지와 방지, 사이버 위협에 대응하기 위한 네트워크 모니터링, 제품과 서비스의 정확성·신뢰성을 유지하기 위한 업데이트가 그런 예입니다. 「개인정보 보호법」 제 15 조 제 1 항 제 6 호는 개인정보처리자의 정당한 이익을 위한 개인정보 처리를 허용하고 있지만, 이는 해당 이익이 정보주체의 권리보다 '명백히 우선하는(manifestly superior)' 경우에 한정됩니다. 이 규정은 그 의미가 분명하지 않을뿐더러, 기업이 해당 근거를 법적 근거로 활용하기 위해서는 상당히 높은 문턱을 넘어야 한다는 뜻으로 읽힙니다.
관련 제도 및 기준	「개인정보 보호법」 제 15 조 제 1 항 제 6 호
문제점	• **'명백히 우선하는'이라는 문턱으로 인해 「개인정보 보호법」 상 정당한 이익에 따른 개인정보 처리의 법적 근거는 다른 주요 국가의 개인정보 체계에 비해 그 인정 범위가 현저히 좁고 경직돼 있습니다.** 예를 들어, 「EU 일반개인정보보호법(**GDPR**)」 제 6 조 제 1 항 (f)는 개인정보처리자의 정당한 이익을 위해 필요한 개인정보 처리를 허용하되, 해당 이익이 정보주체의 이익이나 기본권·자유에 우선하지 못하는 경우에만 이를 배제합니다. 마찬가지로 싱가포르의 「개인정보보호법(**PDPA**)」에 따르면, 조직 또는 다른 사람의 '정당한 이익이 개인에게 미치는 부정적인 영향을 상회하는 경우', 조직은 동의 없이도 개인정보를 수집·이용 또는 공개할 수 있습니다. 그 결과 EU 나 싱가포르에서는 기업이 이 근거를 활용하기가 수월하고, 동시에 개인정보 침해 위험을 줄이도록 관행을 개선할 유인도 분명합니다. 반면 한국에 위치한 기업은 더 엄격하고 예측하기 어려운 기준을 마주합니다. • **이와 관련하여, 기업은 자신의 정당한 이익이 '명백히 우선하는' 것으로 인정될지 여부를 사전에 판단하기 어렵기에, 모든 개인정보 처리 활동에 있어 동의에 지나치게 의존하는 경향이 있습니다.** 그만큼 개인에게는 점점 더 많은 동의 요청이 쌓이게 되고, '동의 피로'가 생기며, 정작 동의가 중요한 의미를 갖는 상황에서 그 가치가 저하됩니다. 동의는 민감정보의 처리나 개인의 합리적인 기대를 명백히 벗어나는 2 차적 이용 등 정보주체의 권리와 이익에 중대한 영향을 미치는 개인정보 처리에 한정하여 요구되어야 합니다. 동의에 대한 지나친 의존은 개인정보의 주체인 정보주체를 보호하기 위한 개인정보 처리마저 위축시키는 결과를 초래합니다. 사기 탐지 및 방지,

	사이버보안 및 네트워크 모니터링, 제품 및 서비스의 정확성과 신뢰성을 확보하기 위한 업데이트는 모두 정보주체에게 직접적인 혜택을 제공하는 활동입니다.[3] 기업이 이러한 개인정보 처리를 앞두고 망설이게 만드는 제도는 개인정보 보호 수준을 향상시키지 못합니다. 오히려 법이 보호하고자 하는 사람들에게 위험을 초래할 수 있습니다. • **동의에 대한 지나친 의존은 책임 있는 AI 개발도 저해할 수 있습니다.** 적법하게 수집한 개인정보라도 정보주체에게 현실적으로 동의를 받기 어렵다면, 기업은 AI 모델 학습이나 개발을 주저하게 됩니다. 정보주체와 연락이 닿기 어려운 대규모 데이터셋이나 과거에 축적된 데이터를 활용하는 연구가 그렇습니다. 또한 특정 집단이 유독 동의를 꺼릴 경우 학습 데이터가 한쪽으로 기울어 표본 편향이 생기고, 결국 대표성이 낮은 집단에서 성능이 떨어지는 AI 가 만들어집니다. 한국 이용자에게 정확하고 공정한 AI 를 만들려면 한국 데이터를 포함한 다양하고 대표성 있는 데이터에 접근할 수 있어야 합니다.
제안내용	**「개인정보 보호법」 제 15 조 제 1 항 제 6 호를 타 주요국의 개인정보 보호법에서 인정하는 정당한 이익에 따른 개인정보 처리 근거에 부합하도록 확대하고, 이를 동의와 대등한 법적 근거로 인정하시기를 제언드립니다.** 이와 같은 근거에 따라 개인정보를 처리하는 경우에는 목적의 정당성, 필요성, 정보주체의 합리적 기대, 잠재적 영향, 보호조치 유무를 함께 따지는 이익형량으로 판단하되, 그 과정에서 위험을 낮추는 조치가 반영되어야 합니다. 요건은 개인정보처리자의 이익이 정보주체의 권리보다 명백히 우선할 것이 아니라, 해당 처리가 정보주체의 권리와 이익을 해치지 않을 것이어야 합니다. 아울러 이렇게 정비한 정당한 이익 근거는 동의의 예외가 아니라 동의와 나란히 서는 처리 근거로 작동해야 합니다.

[3] EU 일반개인정보보호법(GDPR)은 전문(Recital) 제 47 호부터 제 49 호에서 이러한 개인정보 처리를 정당한 이익에 따른 처리로 명시적으로 인정하고 있습니다.

제언사항 2: 개인정보처리 "위탁자"와 "수탁자"의 책임의 명확한 구분

현황 및 상황 (문제 사례)	「개인정보 보호법」은 개인정보를 처리하는 주체를 두 가지로 구분하고 있습니다. 첫째는 제 2 조제 5 호의 '개인정보처리자(personal information controller)'로, 업무를 목적으로 개인정보를 직·간접적으로 처리하는 주체입니다. 이 가운데 제 26 조에 따라 개인정보 처리 업무를 위탁한 자를 '위탁자'라 합니다. 둘째는 제 26 조의 '수탁자(outsourcee)'로, 위탁자로부터 개인정보 처리를 위탁받아 그 지시에 따라 개인정보를 처리하는 주체를 의미합니다. **중요한 점은 두 주체가 다름에도 불구하고 보호법상 의무는 양쪽에 동일하게 지운다는 점입니다. 동의를 받을 의무, 유출 사실을 정보주체에게 알릴 의무, 열람·삭제·전송 요구에 대응할 의무가 모두 그렇습니다.** 두 주체의 역할과 의무가 실질적으로 구분되지 않는다면 소비자와 기업 모두 불확실성이 커지며, 애초에 두 주체를 나눠 정의한 취지도 무색해집니다. 소비자는 누가 자기 정보를 지킬 책임이 있고 권리를 어디에 행사해야 하는지 알기 어렵고, 기업은 자신에게 적용되는 의무의 윤곽을 잡기 어려워 책임 소재와 준수 양면에서 공백이 생길 가능성이 있습니다.
관련 제도 및 기준	「개인정보 보호법」 제 2 조 제 5 호, 제 26 조
문제점	• **'수탁자'에게 부과되는 의무의 상당수는 소비자를 직접 상대하는 의무로서, 수탁자가 이를 적절히 이행하기 어려운 경우가 많습니다.** 동의를 받거나, 정보주체에게 통지하거나, 정보주체의 권리 행사 요구에 대응하는 등의 의무는 해당 주체가 어떠한 개인정보를 보유하고 있는지 파악하고 있으며, 해당 정보주체를 식별하여 직접 소통할 수 있다는 전제를 바탕으로 합니다. 그러나 수탁자가 항상 이러한 요건을 충족하는 것은 아닙니다. 예를 들어, 많은 기업용 클라우드 및 서비스형 소프트웨어(SaaS) 제공업체는 '수탁자'로서 고객(즉, '위탁자')의 지시에 따라서만 개인정보를 처리합니다. '수탁자'는 계약상 해당 데이터에 일절 접근할 수 없도록 제한되는 경우가 많으며, 해당 데이터의 내용을 알지 못할 수 있고, 해당 데이터가 누구와 관련된 것인지 확인할 수 있는 수단도 없습니다. '수탁자'에게 소비자를 직접 상대하는 의무를 이행하도록 요구하는 것은 오히려 개인정보 보호를 저해할 수 있습니다. 이는 수탁자가 본래라면 전혀 열람하거나 검토하지 않을 데이터를 부득이하게 접근·분석해야 하며, 본인 확인이 되지 않은 요청자에게 개인정보를 제공할 위험이 있기 때문입니다. 반면, 개인정보처리자 중 위탁자는 개인정보가 어떠한 목적으로, 어떠한 방식으로 수집·이용되는지를 결정하고 정보주체와 직접적인 관계를 맺고 있습니다. 해당 주체는

	자신이 어떠한 개인정보를 수집하였는지 파악하고 있으며, 요청을 제기한 정보주체의 신원을 확인하고 그 처리 결과를 해당 정보주체에게 전달할 수 있습니다. 따라서 개인정보보호법상 소비자를 직접 상대하는 의무는 개인정보처리자 중 '위탁자'가 부담하는 것이 가장 적절합니다. • **이와 관련하여, 두 주체에 동일한 의무를 부과하는 것은 국제적 기준에 부합하지 않으며, AI 시대의 데이터 생태계에도 맞지 않습니다.** 각국 개인정보 보호법은 처리의 목적과 수단을 정하는 컨트롤러(data controller)와 컨트롤러의 지시에 따라 개인정보를 처리하는 프로세서(data processor)를 구분하고, 각자가 실제로 이행할 수 있는 의무를 나눠 지웁니다. GDPR 은 정보주체를 직접 상대하는 의무를 컨트롤러에 지우고, 프로세서에는 컨트롤러의 문서화된 지시에 따라 처리할 의무, 컨트롤러를 지원할 의무, 자신이 보유한 개인정보를 안전하게 지킬 의무를 지웁니다. 싱가포르 PDPA 와 미국 캘리포니아 「소비자 프라이버시법」(CCPA)도 마찬가지입니다. 두 역할을 나눠 정의하면서 의무는 똑같이 부과하는 한국의 보호법은 국제적으로 이례적입니다. 국제적으로 통용되는 역할 분담을 전제로 보호 체계와 계약, 기술 구조를 설계해 온 기업으로서는 준수 부담이 그만큼 커집니다.
제안내용	• **국제기준에 부합하도록 정의를 재정비할 것을 제언드립니다.** '위탁자'는 "단독으로 또는 다른 주체와 공동으로 개인정보의 처리 목적과 수단을 **결정하는** 주체"로 정의하고, '수탁자'는 "위탁자를 대신하여 개인정보를 처리하는 주체"로 정의하도록 조정해야 합니다. 이를 통해 양 주체의 역할을 명확히 구분할 수 있으며, 결과적으로 양 주체 간 책임과 의무를 보다 정확하게 배분할 수 있습니다. • **'위탁자'와 '수탁자'의 의무를 각 주체의 역할에 따라 적절하게 배분해 주실 것을 제언드립니다.** 특히 개인으로부터 동의를 받거나 정보주체의 권리 행사 요구에 대응하는 등 소비자를 직접 상대하는 의무는 '수탁자'가 아닌 '위탁자'에게 부과되어야 합니다. 이는 개인정보처리자 중 위탁자가 소비자의 개인정보를 어떠한 방식과 목적으로 수집할지를 결정하는 주체라는 점을 반영한 것입니다. 반면 '수탁자'에게는 개인정보를 안전하게 보호하고, 위탁자를 대신하여 지시에 따라 개인정보를 처리하는 등 그 역할에 부합하는 의무가 부과되어야 합니다. 이러한 책임과 의무의 배분은 국제적인 기준에도 부합합니다.

제언사항 3: 국경 간 데이터 이전 절차 개선

현황 및 상황 (문제 사례)	「개인정보 보호법」은 제 28 조의 8 을 통해 개인정보의 국외 이전을 규율하고 있습니다. 개인정보의 국외 이전은 다음의 5 가지 법적 근거 중 하나에 해당하는 경우를 제외하고는 금지됩니다. ① 정보주체로부터 국외 이전에 관한 별도의 동의를 받은 경우, ② 법률, 대한민국을 당사자로 하는 조약 또는 그 밖의 국제협정에 개인정보의 국외 이전에 관한 특별한 규정이 있는 경우, ③ 정보주체와의 계약을 체결하거나 이행하기 위해 국외 이전이 필요하고, 관련 법령에서 정한 사항을 개인정보처리방침에 공개하거나 정보주체에게 고지한 경우, ④ 개인정보 이전을 받는 자가 개인정보보호위원회가 정하여 고시한 인증을 보유하고 필요한 보호조치를 취한 경우, 또는 ⑤ 개인정보가 이전되는 국가 또는 국제기구가 개인정보보호위원회에 의해 개인정보보호법과 실질적으로 동등한 수준의 보호를 제공하는 것으로 인정된 경우입니다. 그러나 실무에서는 여러 이유로 국외 이전이 여전히 어렵습니다(아래 '문제점' 참조). 글로벌 서비스를 제공하는 기업들이 AI 개발과 학습을 위해 국외 이전에 점점 더 의존하고 있다는 점을 감안한다면 더욱 그렇습니다.
관련 제도 및 기준	「개인정보 보호법」 제 28 조의 8
문제점	• **동의에 의한 국외 이전은 실효성이 낮고 정보주체 보호에도 큰 도움이 되지 않습니다.** 국외 이전이 동의에 근거하는 경우, 해당 이전이 개인정보를 수집한 본래의 목적을 달성하기 위해 필요하고 정보주체가 이미 해당 개인정보 처리에 동의한 경우에도, 개인정보처리자는 국외 이전에 대해 별도의 동의를 받아야 합니다. 또한 동의를 받기 전에 개인정보처리자는 제 28 조의 8 제 2 항에 따라 개인정보의 항목, 이전되는 국가, 이전 시기 및 방법, 이전받는 자의 성명(법인인 경우에는 그 명칭 및 연락처) 등 정해진 사항을 정보주체에게 알려야 합니다. 그러나 이전 시기와 같은 정보는 국외 이전이 자신의 개인정보에 어떠한 영향을 미치는지를 정보주체가 이해하는 데 실질적인 의미가 크지 않습니다. 또한 이전받는 법인의 명칭과 담당자의 정보를 개인정보처리방침에 기재하도록 하는 것은 해당 정보가 변경될 수 있고 사전에 쉽게 확인하기 어려울 수 있다는 점에서 현실적이지 않습니다. 결국 위와 같은 요건이 결합되면서 정보주체에게 과도한 동의 요청과 세부 정보를 제공하게 되고, 이는 동의 피로를 가중시키며, 개인정보 보호에는 실질적으로 기여하지 못합니다. 나아가 기업의 운영 비용도 증가시킵니다. • **대안이 되는 국외 이전 메커니즘은 국제 관행에 비해 그 범위가 제한적입니다.** 이전 기업과 국외 수령자가 맺는 독립된 계약형 수단, 예컨대 SCC(표준계약조항)는 이전 근거로 인정되지 않습니다. 이에,

	이러한 수단을 축으로 글로벌 준수 체계를 갖춘 기업도 한국에서는 이를 쓸 수 없고, 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증처럼 한국에서만 통용되는 인증을 받은 수령자에게만 이전하는 식의 대안을 찾아야 합니다. • **동등성 인정 경로는 절차가 느리고 예측 가능성이 낮습니다.** 2025 년 9 월 유럽연합(EU)에 대한 동등성 인정은 개인정보보호위원회가 개인정보보호법 제 28 조의 8 제 1 항 제 5 호에 따라 내린 최초의 동등성 인정 결정이었으며, 현재까지 유일한 결정으로 남아 있습니다. 다른 국가에 대한 심사 일정이 제시되어 있지 않고, 국가별 우선순위에 대한 기준이나 방법론도 공개되어 있지 않으며, 한국 경제에 중요한 국가가 어디인지에 대해 업계가 의견을 제시할 수 있는 절차도 마련되어 있지 않습니다. 또한 이러한 심사 방식은 개인정보를 효과적으로 보호하면서도 미국과 같이 입법 구조가 상이한 국가에 불리하게 작용할 우려가 있습니다. 미국은 포괄적인 단일 법률 대신 주 단위 개인정보 보호법과 연방의 분야별 규제를 결합해 개인정보의 상업적 수집·이용을 규율합니다. 포괄적 법률의 유무가 아니라 관련 법·제도 전반을 놓고 판단하지 않는다면, 이런 국가로의 이전은 사실상 무기한 동등성 경로 밖에 놓이게 됩니다. • **종합적으로 보았을 때, 위와 같은 문제들이 겹치면서, 한국의 개인정보 국외 이전 제도와 관련한 문제는 글로벌 서비스를 제공하는 기업에 상당한 비용과 부담을 초래합니다.** AI 시대에는 그 무게가 더 커집니다. AI 시스템의 개발과 학습은 개인정보를 포함한 데이터를 국경 너머로 대규모로 옮길 수 있는지에 달려 있기 때문입니다.
제안내용	• **'별도 동의' 요건을 조정할 것을 제언드립니다.** 개인정보의 국외 이전이 해당 개인정보를 수집한 목적을 달성하기 위해 필요한 경우에는 최초의 개인정보 처리 동의만으로도 해당 국외 이전의 법적 근거로 충분하도록 하고, 제 28 조의 8 제 1 항 제 1 호에 따른 '별도 동의'를 요구하지 않아야 합니다. 이는 EU 일반개인정보보호법(GDPR)의 접근 방식과도 부합합니다. • **제 28 조의 8 제 1 항 제 4 호의 인증 절차를 통해 추가적인 국외 이전 수단을 인정해주실 것을 제언드립니다.** 개인정보보호위원회는 EU SCC, 영국 국제 데이터 이전 계약(UK International Data Transfer Agreements), 글로벌 및 APEC CBPR, ASEAN 모델 계약조항(ASEAN Model Contractual Clauses), ISO/IEC 27701 등 국제적으로 인정되는 국외 이전 수단을 인정해야 합니다. 많은 글로벌 기업들은 국가 간 개인정보를 이전하는 과정에서 개인정보를 보호하기 위해 위와 같은 수단을 활용하고 있으며, 위 수단들은 해외 수령자에게 개인정보보호법이 요구하는 사항과도 상당 부분 공통점을 갖고 있습니다. 이를 인정할 경우, 기업은 별도의 동의나 한국 전용 인증

	없이도 한국에서 개인정보를 이전하거나 한국의 개인정보를 제공받을 수 있게 됩니다. 나아가, 인정된 여러 수단 가운데 자사 사업에 가장 맞는 방식을 고를 수 있어 운영상 유연성도 커집니다. 더불어 법적 불확실성이 줄고, 글로벌 서비스를 제공하는 국내외 기업의 준수 부담이 완화되며, 여러 이전 수단을 함께 두는 다른 국가 제도와도 발을 맞출 수 있게 됩니다. • **제 28 조의 8 제 1 항 제 5 호에 따른 동등성 인정 절차의 예측 가능성을 높여 주실 것을 제언드립니다.** 개인정보보호위원회는 다른 국가의 개인정보 보호 수준을 심사하는 데 필요한 기간을 명확히 규정하고, 심사 대상 국가의 우선순위를 정하는 기준과 방법론을 공개하며, 어떤 국가를 우선적으로 심사해야 하는지에 대해 업계의 의견을 수렴해야 합니다. 또한 동등성 심사를 수행할 때에는 단일한 포괄적 개인정보 보호법의 존재 여부에만 초점을 맞추기보다는, 해당 국가에서 개인정보를 보호하는 관련 법률 및 규제 체계 전반을 종합적으로 고려해야 합니다. 이를 통해 주(州) 단위의 개인정보 보호법과 연방 차원의 분야별 규제를 통해 개인정보를 보호하는 국가가 동등성 인정 절차를 이용하지 못하는 상황이 발생하지 않도록 해야 합니다.

마치며

BSA는 한국의 개인정보 보호 제도를 종합적으로 검토하는 이번 과정에 의견을 낼 기회를 주신 위원회에 감사드립니다. BSA는 개인정보를 실효적으로 보호하면서 책임 있는 데이터 활용도 가능하게 하려는 위원회의 노력을 지지합니다. 본 의견서에서 제시한 내용에 관해 더 논의할 기회가 있기를 바라며, 검토가 진행되는 동안 언제든 필요한 자료와 도움을 드리겠습니다. 본 의견서에서 제언드린 사안에 대해 궁금하신 점이 있거나 논의가 필요하시면 언제든지 연락 주시기 바랍니다.

감사합니다.

Tham Shen Hong
Director, Policy – APAC