2026 년 7 월 13 일

# 개인정보 보호법 시행령 일부개정령(안)에 관한
# BUSINESS SOFTWARE ALLIANCE(BSA) 의견서

**개인정보보호위원회 귀중**

BSA [1] (비즈니스 소프트웨어 연합, Business Software Alliance, 이하 "BSA")은 개인정보보호위원회의 「개인정보 보호법 시행령 일부개정령(안)」(이하 "시행령 개정안")에 대하여 의견을 제출할 기회를 주신 데 대해 감사드립니다.

BSA 는 전 세계 정부와 시장을 대상으로 글로벌 소프트웨어 산업을 대변하고 있습니다. BSA 회원사들은 클라우드 스토리지 서비스, 고객관계관리(CRM) 소프트웨어, 인적자원관리 프로그램, ID 관리 서비스, 보안 솔루션, 협업 소프트웨어 등 다양한 기업 활동을 지원하는 기술 제품과 서비스를 개발·제공하고 있습니다. 아울러 BSA 회원사들은 한국 경제 전반에 제품과 솔루션을 공급해 왔으며, 한국 기업들이 이를 바탕으로 사업을 운영하고 성장시켜 나가고 있다는 점을 매우 뜻깊게 생각합니다.

BSA 는 개인정보 보호법과 그 시행령의 발전 과정에 꾸준히 관심을 기울여 왔으며, 관련 의견 수렴 절차에도 적극적으로 참여해 왔습니다[2]. 이번 시행령 개정안은 2026 년 3 월 공포된 개정 개인정보 보호법(이하 "2026 년 개정법")을 구체적으로 이행하기 위한 내용을 담고 있습니다. 2026 년 개정법은 산업계에 부과되는 개인정보 보호 의무를 대폭 강화하는 한편, 위반 시 적용되는 제재 수준 역시 크게 상향하였습니다. 이에 BSA 는 시행령 개정안이 기업이 준수해야 할 사항을 명확하고 실효성 있게 제시하는 동시에, 기업이 이미 구축·운영하고 있는 정보보호 및 개인정보 보호 체계에 대한 투자와 노력을 적절히 반영할 수 있도록 아래 사항을 검토해 주실 것을 제언드립니다.

---

[1] 1BSA 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: 개인정보 보호법 시행령안에 대한 BSA 의견서(2023 년 6 월), (개인정보 보호법 개정안에 대한 BSA 의견서, 2021 년 11 월)

## 요약

다음과 같은 내용을 제언드립니다.

### 1. 정보보호 및 개인정보보호 관리체계(ISMS-P) 의무 인증 요건

- 수탁자가 개인정보처리자(위탁자)의 위탁을 받아 처리하는 개인정보는 제 34 조의 9 제 4 호에 따른 ISMS-P 인증 의무 대상 판단 기준에 포함되지 않도록 명확히 규정해야 합니다.
- ISO/IEC 27001, 서비스 조직 통제 2(SOC 2), ISO/IEC 27701, 유럽연합 일반 개인정보 보호법(GDPR), 글로벌/APEC 국경 간 개인정보 보호 규칙(CBPR) 체계 등 국제적으로 인정받는 보안·개인정보보호 인증을 이미 보유한 기업이 전면적인 중복 심사를 거치지 않고 기존 인증 체계를 토대로 ISMS-P 인증을 취득할 수 있도록 명확한 절차를 마련해야 합니다.

### 2. 통지 의무의 범위 및 기준

- 단순히 유출 "가능성"이 있다는 이유만으로 정보주체에 대한 통지 의무를 부과해서는 안 됩니다. 통지가 요구되는 경우는 정보주체에게 중대한 피해를 초래할 실질적 위험이 있는 사고로 한정되어야 하며, "객관적 정황"과 "높은 가능성"의 의미를 구체적이고 명확한 예시와 함께 제시해야 합니다.
- 개인정보의 위조·변조 또는 훼손에 대한 통지·신고 의무는 해당 사고가 기술적으로 발생했다는 사실만으로 발동되어서는 안 되며, 그 사고가 정보주체의 권익에 실질적인 침해 위험을 초래하는 경우로 한정해야 합니다.

### 3. 제재 체계

- 개인정보 보호법 제 64 조의 2(과징금의 부과) 제 6 항에 따른 감경 여부를 판단할 때, 기업이 개인정보 보호에 투입한 투자의 규모와 지속성뿐 아니라 유출 사고를 일으킨 공격 주체의 성격과 공격 수법의 정교성도 고려 요소로 명시해야 합니다. 또한 유출 사고 당시 통용되던 업계 표준에 부합하는 보안 조치를 취하였음을 입증한 경우, 이를 유력한 감경 사유로 고려하도록 명시해야 합니다.
- 개정법상 의무가 시행된 후 최소 12 개월의 유예기간을 두어, 기업이 새로운 요구사항에 맞추어 컴플라이언스 체계를 정비할 충분한 시간을 확보할 수 있도록 해야 합니다.

## ISMS-P 인증 의무화

2026 년 개정법에 따라 ISMS-P 인증은 종전의 완전 자율 제도에서, 시행령으로 정하는 매출액 및 개인정보 처리 규모 기준을 충족하는 개인정보처리자에게 전면 의무화되는 제도로 전환되었습니다. 특히 인증 의무 대상은 "전년도 매출액 1 조 원 이상, 정보통신서비스 부문 전년도 매출액 100 억 원 이상, 국내 정보주체 수 일일 평균 3 천만 명 이상"의 요건을 모두 충족하는 대규모 개인정보처리자까지 확대됩니다.[3]

BSA 는 인증 의무 대상의 범위가 구체적인 수치 기준으로 설정되어 기업이 ISMS-P 인증 의무의 적용 여부를 보다 명확하게 예측할 수 있게 된 점을 긍정적으로 평가합니다. 다만 다음 사항은 여전히 해소되지 않은 채 남아 있습니다.

### 정보주체 수 기준은 개인정보처리자(위탁자)에게만 적용되어야 합니다

시행령 개정안은 인증 의무 대상 기준으로 "국내 정보주체 수 일일 평균 3 천만 명 이상"을 규정하고 있습니다.

그러나 이 기준은 개인정보 보호법상 "위탁자"가 아닌 "수탁자"로 기능하는 기업에는 적용하기 어렵습니다. 각국의 개인정보보호 제도는 개인정보의 처리 목적과 수단을 결정하는 위탁자와, 위탁자를 대신하여 그 지시에 따라 개인정보를 처리하는 수탁자를 구분하고 있습니다[4]. 우리 개인정보 보호법도 이 두 역할을 구분하여 정의하고는 있으나, 개인정보를 왜, 어떻게 처리할지 결정하는 주체(위탁자)와 그렇지 않은 주체(수탁자)에게 서로 다른 의무를 지우는 다른 나라들과 달리, 양자에게 사실상 동일한 의무를 부과한다는 점에서 차이가 있습니다[5].

따라서 시행령 개정안의 기준은 개인정보의 처리 목적과 방법을 결정하고, 그에 따라 자신이 매일 처리하는 국내 정보주체의 수를 파악할 수 있는 지위에 있는 위탁자에게만 적용되어야 합니다. 수탁자는 이러한 정보를 알지 못할 수 있기 때문입니다[6]. 예를 들어 기업용 클라우드 및 서비스형 소프트웨어(SaaS) 제공자는 통상 기업 고객의 지시에 엄격히 따라 개인정보를 처리하며, 이때 개인정보의 처리 목적과 방법을 결정하고 정보주체와 직접적인 관계를 유지하는 주체는 그 기업 고객, 즉 위탁자입니다. 이러한 제공자는

---

[3] 시행령(안) 제 34 조의 9. 그 밖에 의무 인증 대상에 포함되는 세 가지 유형의 개인정보처리자는 다음과 같습니다. 제 30 조의 2 에 따른 공공시스템운영기관 중 보호위원회가 정하여 고시하는 자, 「전파법」 제 10 조에 따라 주파수를 할당받아 이동통신서비스를 제공하는 자로서 정보주체와 이동통신서비스의 이용에 관한 계약을 체결한 자, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 23 조의 3 제 1 항에 따른 본인확인기관

[4] Controllers and Processors: A Longstanding Distinction in Privacy, April 2025, https://www.bsa.org/policy-filings/controllers-and-processors-a-longstanding-distinction-in-privacy.

[5] 개인정보 보호법 26 조

[6] 예를 들어, 오직 개인정보 처리자의 지시에 따라서 개인정보를 처리하고, 계약상 해당 정보를 다른 목적으로 접근하거나 이용하는 것이 금지될 수 있는 개인정보 수탁자는 대개 자신이 처리하는 데이터의 내용이나 해당 데이터와 관련이 되어 있는 구체적인 인물들이 누구인지 또는 특정 정보주체의 신원을 확인할 수 있는 위치에 있지 않은 경우가 많습니다. 반면 개인정보 처리자(위탁자)는 어떤 데이터를 수집할지, 어떤 목적으로 수집·이용할지를 결정하며, 정보주체와 직접적인 관계를 유지합니다.

수탁자의 지위에서 전체 고객군에 걸쳐 대량의 데이터를 처리할 수는 있으나, 일반적으로 해당 데이터의 이용 방식에 대한 독자적인 권한이 없고 정보주체와의 직접적인 관계도 없으며, 많은 경우 기준 산정을 위해 어느 정보주체가 국내 정보주체인지 식별할 현실적인 방법조차 없습니다. 만약 수탁자가 여러 위탁자를 대신하여 처리하는 데이터가 제 34 조의 9 제 4 호의 기준에 산입된다면, 아무런 권한도 정보주체와의 직접적 관계도 없는 기업에 인증 의무가 부과되는 반면, 정작 실질적인 권한과 정보주체와의 직접적 관계를 보유한 위탁자는 적용 대상에서 제외되는 결과가 초래될 우려가 있습니다.

**정책 제언:** 위탁자의 지시에 따라 수탁자가 처리하는 개인정보는 제 34 조의 9 제 4 호에 따른 ISMS-P 인증 의무 대상 판단 기준에 포함되지 않도록 규정해 주실 것을 제언드립니다.

## 산업계가 기존의 국제 표준과 인증을 활용할 수 있도록 해야 합니다

현행 개정안이 다루지 않은 또 다른 문제는, 주요 국제 표준에 따라 이미 엄격한 보안·개인정보보호 체계를 구축하고 독립적인 감사까지 거친 기업을 이번 인증 의무에서 어떻게 다룰 것인가입니다. 이러한 기업들은 대체로 ISO/IEC 27001 인증과 SOC 2 보고서 등 국제적으로 인정받는 보안 인증은 물론, ISO/IEC 27701, EU GDPR, 글로벌/APEC CBPR 체계와 같은 개인정보보호 프레임워크를 중심으로 전 세계에 걸친 컴플라이언스 체계를 갖추고 있습니다.

이러한 국제 인증·표준은 ISMS-P 의 요구사항과 상당 부분 공통된 기반을 공유합니다. 따라서 ISO/IEC 27001 수준의 보안 관리 체계나 GDPR·CBPR 수준의 개인정보 거버넌스 체계를 이미 구축하고 독립적인 감사까지 거친 기업이라면, ISMS-P 심사가 확인하고자 하는 사항의 상당 부분을 사실상 이미 이행하고 있는 셈입니다. 이러한 기존 체계를 인정하지 않은 채 처음부터 끝까지 전면적인 ISMS-P 심사를 다시 받도록 의무화하는 것은 불필요한 중복이며, 실질적인 개인정보 보호 수준의 향상이라는 실익 없이 비용과 행정 부담만 늘릴 뿐입니다. 그 결과 한국의 정부기관과 기업이 더 비싸고 기능은 떨어지며 보안성마저 낮은 서비스만을 이용하게 될 수도 있습니다.

아울러 BSA 는 개인정보보호위원회가 ISMS-P 요구사항을 클라우드 보안인증(CSAP), 공공부문 클라우드 서비스에 대한 국가정보원 주관 통합 보안 체계로의 이행 움직임 등 국내 정보보안 인증 제도의 관련 동향과 조율하여, 동일한 클라우드 서비스에 중복되거나 상충하는 인증 요구사항이 적용되지 않도록 해 주실 것을 제언드립니다.

**정책 제언:** ISO/IEC 27001, SOC 2, ISO/IEC 27701, GDPR, 글로벌/APEC CBPR 체계 등의 인증과 절차를 이미 갖춘 기업이 전면적인 중복 심사를 거치지 않고도 기존 인증 및 프레임워크를 토대로 ISMS-P 인증을 취득할 수 있도록 명확한 절차를 마련해 주실 것을 제언드립니다.

## 통지 의무의 범위 및 적용 기준

개정 개인정보 보호법은 개인정보 유출이 확인된 경우는 물론, 유출이 발생했을 "가능성"이 있는 경우에도 정보주체에게 통지하도록 요구합니다. 그러나 이러한 방식은 실제로 일어나지 않았을 수도 있는 사고에 관한 정보까지 정보주체에게 제공하게 되어, 정작 실제 유출로 인한 피해 통지를 정보주체가 가려내거나 주목하기 어렵게 만들 수 있습니다. BSA 는 바로 이 점을 우려합니다.

시행령 개정안은 이 의무를 구체화하면서 통지 요건을 발동시키는 두 가지 상황을 규정하고 있습니다. 첫째, 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 불법적인 접근을 알게 된 경우로서, 개인정보가 유출 등이 된 객관적인 정황은 있으나 유출 등이 된 정보주체를 특정하기 곤란한 경우입니다. 둘째, 개인정보처리자가 처리하는 개인정보가 불법적으로 거래·유통되고 있다는 사실이 객관적으로 확인된 경우로서, 유출 등이 확인된 정보주체 이외의 정보주체에 관한 개인정보도 유출 등의 "가능성이 높다"고 인정되는 경우입니다[7].

아울러 개정안은 통지 의무를 발생시키는 사고의 범위 자체도 확대합니다. 현행 규정상 통지 대상 사고는 개인정보의 분실·도난·유출로 한정되어 있으나, 개정안은 그 범위를 "개인정보의 위조·변조 또는 훼손[8]"까지 넓히고 있습니다. BSA 는 이러한 점들에 대해 다음과 같은 우려를 가지고 있습니다.

### "가능성" 기준은 삭제하거나, 구체적인 중대한 피해 발생과 연계해야 합니다

일반 원칙으로서, 단지 유출 가능성이 있다는 사정만으로 통지를 요구해서는 안 됩니다. 유출 가능성만으로 기업에 정보주체 통지를 강제할 경우 다음과 같은 여러 우려스러운 결과가 초래될 수 있습니다.

- 기업은 해당 사고가 결과적으로 개인정보 침해로 이어지지 않는 경우에도 예방적 차원에서 불필요한 통지를 하게 될 수 있습니다. 명확하지 않은 기준에 따른 과잉 통지는 시행령 개정안의 취지에 반할 뿐 아니라, 정보주체가 통지 전반에 무감각해지게 하여 실제로 중대한 침해 사고가 발생했을 때 이를 가려내고 적절히 대응하기 어렵게 만들 수 있습니다.
- 어떤 증거나 징후가 있어야 통지 요건이 충족되는지에 관한 명확한 지침이 없어, 기업마다 일관되지 않은 기준을 적용할 수 있습니다. 실질적으로 유사한 사실관계에 직면한 기업들이 요건 충족 여부에 대해 서로 다른 결론에 이를 수 있고, 이는 업계 전반의 관행을 들쭉날쭉하게 만들며 예측 불가능한 집행 결과로 이어집니다. 이러한

[7] 시행령 개정안 제 39 조 제 2 항

[8] 시행령 개정안 제 30 조의 2 제 2 항제 1 호

불확실성은 대폭 상향된 과징금 규모로 인해 한층 커지며, 결국 기업으로서는 사후에 위반으로 판정될 위험을 피하기 위해 과도하게 통지하는 쪽으로 기울 강한 유인을 갖게 됩니다.

- 유출 가능성만으로 통지를 요구하면, 자원이 가장 필요한 순간에 그 자원이 분산됩니다. 불법적 접근을 탐지한 직후에는 기업의 보안·컴플라이언스 인력에 여유가 없기 마련이며, 이때 그 역량은 사고를 차단하고 실제 피해 범위를 파악하며 피해를 복구하는 데 집중되어야 합니다. 그러나 유출 가능성까지 통지하도록 요구하면, 기업은 사고 해결이라는 기술적·운영적 작업에 집중해야 할 인력을 불확실한 기준에 따른 통지 여부 판단을 문서화하고 정당화하는 데 나누어 쓸 수밖에 없습니다. 신속성과 집중이 무엇보다 중요한 시점에 노력이 엉뚱한 곳에 배분되는 것입니다.
- 확인되지 않은 사고를 성급하게 공개하면 의도치 않게 공격자를 도울 수 있습니다. 사고의 실제 발생 여부를 기업이 확인하기도 전에 통지가 이루어지면, 사이버 범죄자에게 자신들의 수법이 얼마나 효과적이었는지 알려주는 단서가 될 수 있습니다. 나아가 이러한 의무는 공격자가 의도적으로 실체 없는 경보를 일으키도록 부추길 위험도 있습니다. 그렇게 함으로써 기업의 자원을 분산시키고, 결정적인 순간에 사고 대응팀의 주의를 다른 곳으로 돌려놓을 수 있기 때문입니다.

<u>정책 제언</u>: 시행령 개정안에 다음 사항을 반영해 주실 것을 제언드립니다.

- "잠재적" 사고만으로 정보주체에 대한 통지를 요구해서는 안 됩니다. 통지는 정보주체에게 중대한 피해를 초래할 실질적 위험이 있는 경우에만 요구되어야 하며, 개정안상의 모든 의무가 이러한 실질적 위험을 야기하는 유출에만 결부되도록 해야 합니다.
- 통지가 요구되는 경우에는 제39조의2상의 "객관적 정황"과 "높은 가능성"의 의미를 명확히 정의하고, 그 정의에 근거하여 통지가 이루어지도록 해야 합니다. 이러한 정의는 각 기준을 충족하는 증거와 징후가 무엇인지 구체적인 예시로 뒷받침되어야 하며, 이 역시 정보주체에게 중대한 피해의 실질적 위험을 초래하는 상황에 초점을 맞추어야 합니다.

## 통지 대상 사고 범위의 확대는 정보주체에 미치는 실제 위험 수준을 반영하지 못합니다

통지 대상 사고의 범위를 "개인정보의 위조·변조 또는 훼손"까지 확대한 것은 중대한 변화입니다. BSA 는 이렇게 확대된 범위에 "실질적 위험 기준(materiality threshold)"이 결부되어 있지 않다는 점, 즉 해당 사고가 정보주체에게 실제로 어떤 위험을 초래하는지와 무관하게 통지 의무가 발동된다는 점을 우려합니다.

실제로 이는 다음과 같은 상황을 의미합니다. 어떤 기업이 개인정보의 가용성에 영향을 준 랜섬웨어 공격을 받았으나 데이터가 실제로 분실·도난·유출되지는 않은 경우(예컨대 데이터가 암호화되어 있었고 백업도 되어 있던 경우), 권한 없는 자가 어떤 정보주체의 정보도 열람·접근하거나 빼내 가지 않았음에도 이 사고가 "개인정보 훼손" 사고로서 통지 대상에 포함될 수 있습니다. 동시에, 일부 기록이 일시적으로 변경되었다가 자동 백업·복구 시스템을 통해 완전히 원상 복구된 데이터베이스 오류와 같은 일상적인 운영상 사고까지도 기술적으로는 같은 정의에 해당할 수 있습니다. 실제 데이터 유출로 이어진 심각한 공격과 완전히 복구된 일상적 시스템 오류를 통지 목적상 동일하게 취급한다면, 정보주체가 주의를 기울여야 할 사고와 그렇지 않은 사고를 구별하는 데 도움이 되지 않을뿐더러, 실질적인 피해 위험이 없는 사고에까지 기업과 개인정보보호위원회의 자원을 분산시킬 우려가 있습니다. 이러한 결과를 피하기 위해서는 " 실질적 위험 기준 "의 도입이 필요합니다.

**정책 제언**: 개인정보의 위조·변조 또는 훼손에 대한 통지·신고 의무가 그러한 사고가 기술적으로 발생했다는 사실만으로 발동되는 것이 아니라, 그 사고가 정보주체의 권익에 실질적인 침해 위험을 초래하는 경우에 한하여 발동되도록 명확히 규정해 주실 것을 제언드립니다. 이와 같이 규정된다면 통지·신고 의무가 정보주체와 개인정보보호위원회의 주의를 실제로 요하는 사고에만 적용될 수 있을 것입니다.

## 제재 체계

2026 년 개정법에 따라 특정한 경우 개인정보 유출 사고에 대한 과징금 상한이 기업 "전체 매출액"의 10%까지 상향되었습니다[9]. 시행령 개정안은 개인정보보호위원회가 과징금을 산정할 때 고려할 수 있는 감경 기준을 도입하였으며, 여기에는 기업이 개인정보 보호에 투입한 투자의 규모와 지속성, 거버넌스 체계의 성숙도, 추가적인 보안 강화 노력 등이 포함됩니다[10]. BSA 는 이러한 감경 기준의 도입을 환영하며, 다음과 같이 개선이 필요한 지점을 제언드리고자 합니다.

### 보안 강화에 투자한 기업과 그렇지 않은 기업을 구분해야 합니다

엄격한 보안 체계를 구축·유지하고, 자격을 갖춘 개인정보·보안 전문 인력을 두며, 보안에 지속적으로 투자해 온 기업이라 하더라도 공격의 피해자가 될 수 있습니다. 이러한 기업은 기본적인 보안 조치조차 갖추지 못하여 유출을 당한 기업과 근본적으로 다릅니다.

[9] 개인정보 보호법 제 64 조의 2 제 2 항에 따르면, "전체 매출액(total revenue)"은 위반 행위와 관련이 없는 매출액을 제외한 기업의 전 세계 매출액을 의미합니다. 이러한 강화된 제재는 다음과 같은 경우에 적용됩니다. 즉, 기업이 고의 또는 중대한 과실에 따른 위반 행위를 하고 3 년 이내에 이를 반복하는 경우; 고의 또는 중대한 과실로 발생한 하나의 침해 사고로 인해 1 천만 명 이상의 정보주체에게 영향을 미치는 경우; 또는 개인정보보호위원회의 시정명령을 이행하지 않은 상태에서 침해 사고가 발생한 경우.

[10] 개정 개인정보 보호법 제 64 조의 2 제 6 항

그럼에도 두 기업을 동일한 제재 체계에서 같게 취급하는 것은 법의 제재 취지에 부합하지 않습니다. 꾸준히 보안에 투자해 온 기업에는 유출을 막기 위해 추가로 취할 수 있었던 실질적 조치가 없었던 반면, 투자를 소홀히 한 기업에는 그러한 여지가 있었기 때문입니다.

개정 개인정보보호법 제 64 조의 2(과징금의 부과) 제 6 항에 따르면, 개인정보보호위원회가 기업의 개인정보 보호 투자를 감경 요소로 "고려할 수 있다"고만 규정할 뿐, 이 요소를 공격 자체의 성격과 견주어 어떻게 형량할지는 정하지 않고 있습니다. 여기서 공격의 성격이란 해당 기업이 정교하고 표적화된 공격, 국가가 배후에 있는 공격, 그 밖에 이례적으로 역량이 높은 공격 주체에 직면했는지 여부 등을 말합니다. 기업이 감당해야 했던 공격의 정교함을 그 기업이 기울인 투자와 함께 명시적으로 반영하지 않는 과징금 감경 체계는, 결국 근본적으로 다른 기업들에 똑같이 무거운 제재 위험을 지우게 됩니다.

따라서 시행령 개정안은 충분한 자원을 들여 엄격한 보안 인프라를 유지하고도 정교한 공격자에게 피해를 입은 기업과, 구조적인 투자 부족이나 방치로 인해 유출이 발생한 기업을 구별해야 합니다.

**정책 제언**: 시행령 개정안에 다음 사항을 검토해 주실 것을 제언드립니다.

- 유출 사고를 일으킨 공격 주체의 성격과 수법의 정교성을 개인정보 보호법 제 64 조의 2 제 6 항에 따른 감경 여부 판단의 고려 요소로 명시하고, 이를 기업이 개인정보 보호에 투입한 투자의 규모·지속성과 함께 형량하도록 해야 합니다.
- 기업이 유출 당시 업계 통상 기준에 부합하는 보안 조치를 유지했음을 입증하는 경우, 최종적으로 유출 피해가 발생했더라도 이를 과징금 감경에 유리한 핵심 요소로 고려하도록 명시적으로 규정해야 합니다.

## 제재에 앞서 충분한 유예기간을 부여해야 합니다

이 절에서 다룬 제재 체계는 개정법상 의무와 함께 2026 년 9 월에 시행됩니다[11]. 기업으로서는 관련 인력을 교육하고, 본 의견서 전반에서 다룬 규제 요구사항에 맞추어 전세계의 침해사고 대응 및 거버넌스 체계를 정비할 시간이 필요합니다. 의무 시행과 동시에, 기업이 바뀐 요구사항을 실무에 반영할 유예기간도 없이 개인정보보호위원회가 강화된 과징금 권한을 곧바로 행사한다면, 준수 의지가 없어서가 아니라 이행에 소요되는 현실적인 시간으로 인해 발생한 미비점을 이유로 기업을 제재하는 결과가 발생할 수 있습니다.

**정책 제언**: 개정법상 의무가 시행된 후 최소 12 개월의 유예기간을 명확히 규정해 주실 것을 제언드립니다. 그렇게 하면 기업은 새로운 요구사항에 맞추어 컴플라이언스 체계를 정비할

[11] ISMS-P 인증 획득 의무화 규정의 경우 2027 년 7 월부터 시행된다는 점에서 예외 조치라는 점을 감안하여 작성하였습니다.

충분한 시간을 확보하고, 개인정보보호위원회는 유예기간 종료 후 완전한 집행 권한을 행사할 수 있을 것입니다.

## 마치며

BSA 는 개인정보보호위원회가 2026 년 개정법을 시행하는 과정에서 산업계와 지속적으로 소통해 주신 데 깊이 감사드리며, 본 의견서가 시행령 개정안을 준비하시는 데 도움이 되기를 바랍니다. 저희의 제언이 2026 년 개정법을 준수해야 하는 기업들에게 명확하고 비례적이며 실행 가능한 규정을 마련하시는 데 조금이나마 보탬이 되기를 희망합니다. 본 의견서에서 제언드린 사안에 대해 궁금하신 점이 있거나 논의가 필요하시면 언제든지 연락 주시기 바랍니다.

감사합니다.

Tham Shen Hong
Director, Policy – APAC