December 2025

NEWSLETTER

개인정보 · DPC 그룹 | Data Privacy & Cybersecurity Group

CONTACT

변호사 **고환경**
T: 02.2191.3057
E: hwankyoung.ko@leeko.com

변호사 **채성희**
T: 02.6386.6622
E: sunghee.chae@leeko.com

변호사 **강민채**
T: 02.772.4674
E: minchae.kang@leeko.com

변호사 **손경민**
T: 02.772.4918
E: kyungmin.son@leeko.com

변호사 **이일신**
T: 02.772.5982
E: ilshin.lee@leeko.com

ISMS · ISMS-P 인증 실효성 강화 방안 주요 내용 및 시사점

개인정보보호위원회와 과학기술정보통신부는 2025. 12. 6. 정보보호 관리체계(ISMS) 및 정보보호·개인정보보호 관리체계(ISMS-P) 인증의 실효성을 강화하기 위한 전면 개편 방안(**본건 개편안**)을 발표하였습니다. 본건 개편안은 최근 인증 보유 기업에서 연이어 발생한 해킹 및 대규모 개인정보 유출 사고에 대응하기 위하여 마련된 것으로, 2025. 9. 부터 개인정보보호위원회가 추진하던 개인정보 안전관리 체계 강화 기조의 연장선상에 있습니다. 이하에서는 그 구체적인 내용을 살펴보겠습니다.

1. 주요 내용

1) ISMS-P 의무화 및 인증 기준 강화

현행 개인정보 보호법 하에서, 개인정보처리자는 ISMS-P 인증을 받을지 여부를 자율적으로 결정할 수 있습니다. 그러나 본건 개편안에 따르면 앞으로 주요 개인정보처리시스템(주요 공공시스템, 통신사, 대규모 플랫폼 등)을 대상으로 ISMS-P 인증을 의무화하는 법 개정이 추진될 예정입니다. 아울러, 통신사 및 대규모 플랫폼 사업자 등 국민에게 미치는 영향이 큰 기업에 대해서는 현행보다 강화된 인증기준이 적용될 예정입니다.

2) 인증 단계별 심사방식 전면 개편

<심사 방식 강화 방안 주요 내용 (안)>

구분	기존	개선
인증신청	관리체계 운영명세서	관리체계 운영명세서 + **인증범위 자산현황 추가**
예비심사	심사팀장 1인 방문 (1일)	① **핵심항목 先 검증,** ② **(ISMS(고위험, 사고기업), ISMS-P) 기술심사 방식 적용** (취약점진단, 모의침투)
	핵심항목 미충족 → 본심사 불가 → (최초인증) 신청 반려, (사후심사) 인증효력 취소	
본심사	서면위주, 샘플링 점검 (5일)	서면점검 + **③ 코어시스템 중심 현장실증형 심사**
사후심사	심사팀장 1인 방문 (1일)	심사팀장 1인 + **결함발생 수준별 심사인력 추가 투입**

* 개인정보보호위원회 2025. 12. 6. 보도자료 발췌

▪ **인증신청 단계 – 신청 시 제출 서류의 확대**

ISMS와 ISMS-P 인증신청 시, 현행 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」(**고시**)는 '정보보호 및 개인정보보호 관리체계 인증 신청서'상 첨부서류로 관리체계 운영명세서를 제출하도록 규정하고 있으나, 향후 인증 범위에 대한 자산현황을 추가로 제출하도록 개정이 추진될 예정입니다.

▪ **예비심사 단계 – 예비심사의 실질화**

예비심사는 인증심사 계약 체결 전 심사팀장이 신청기관을 방문하여 인증심사에 필요한 기초자료 구비 유무, 인증심사 준비상태 및 운영여부 등을 예비적으로 확인하는 단계입니다. 본건 개편안은 향후 예비심사 단계를 보다 실질화하는 것을 내용으로 하는바, i) 예비심사 단계에서 핵심항목을 사전에 검증하게 하고, ii) 핵심항목을 충족하지 못한 경우 인증 신청을 반려할 수 있게 하며, iii) ISMS(고위험·사고기업) 및 ISMS-P 인증 대상 기업에 대해서는 취약점 진단, 모의침투 등 기술심사 방식을 적용하게 할 예정입니다.

▪ **본심사 단계 – 현장실증형 심사 강화**

본심사는 서면 위주·샘플링 위주 점검에서 벗어나, 코어시스템을 중심으로 실제 운영환경을 검증하는 현장실증형 심사 방식으로 전환될 예정입니다. 이에 따라 정보보호 관리체계가 문서상으로 적정하게 구축되어 있는지 여부가 아니라, 실제 시스템 및 운영 프로세스가 인증 기준에 맞게 작동하고 있는지를 중심으로 평가가 이루어지게 됩니다.

▪ **사후심사 단계**

현행 규정상으로 사후심사는 인증기업의 신청에 따라 연 1회 이루어지나, 본건 개편안에 따르면 인증기업에서 개인정보 유출사고가 발생한 경우에는 즉시 특별 사후심사를 실시할 수 있도록 관련 규정이 개정될 예정입니다. 이러한 특별 사후심사에서는 심사 인력과 기간이 기존 대비 2배로 확대되며, 사고 원인과 재발 방지 조치, 인증기준 충족 여부 등에 대한 집중 점검이 이루어질 것으로 보입니다. 이 과정에서 핵심항목 미충족 등 중대한 결함이 발견되는 경우, 인증위원회의 심의 · 의결을 거쳐 인증이 취소될 수 있게 됩니다.

사후심사의 실무에 있어서도, 심사팀장 1인이 방문하여 진행하던 방식에서, 결함 발생 수준에 따라 추가 심사 인력을 투입할 수 있도록 심사 인력과 방식이 강화될 예정입니다. 이를 통해 인증 유지 단계에서도 인증기준 충족 여부를 보다 면밀하게 확인할 수 있게 됩니다.

2. 향후 일정

본건 개편안은 과학기술정보통신부 · 개인정보보호위원회 · 인증기관 합동 제도개선 TF에서 최종 확정될 예정이며, 2026년 1분기 중 고시를 개정하는 것을 시작으로, 「개인정보 보호법」 및 「정보통신망의 이용촉진 및 정보보호 등에 관한 법률」의 개정까지 단계적으로 추진될 것으로 보입니다. 2025. 9. 발표된 개인정보보호위원회의 '개인정보 안전관리 체계 강화 방안'에 따르면, ISMS-P의 의무화는 2026년 하반기까지 완료하는 것을 목표로 합니다.

3. 시사점

본건 개편안은 ISMS · ISMS-P 인증제도 전 과정에서 인증기준 충족 여부에 관한 검증을 강화하고, 현장 중심 점검을 확대하는 것을 핵심으로 하고 있으며, 이에 따라 향후 인증 취득·유지의 난이도가 이전보다 높아질 것으로 예상됩니다. 특히 예비심사에서부터 기술심사가 도입되고, 본심사에서 실제 운영환경 기반의 점검이 강화됨에 따라, 기업은 관리체계 전반의 기술적·관리적 취약 요소를 사전에 점검하고 필요한 개선 조치를 마련할 필요가 있습니다.

또한, 사고기업에 대한 특별 사후심사 제도가 새롭게 도입되면, 유출사고 발생 시 기업들은 유출사고에 대한 규제기관의 조사뿐 아니라 특별 사후심사에도 대응하여야 하므로 관련한 업무부담 및 리스크가 현저히 증가할 것으로 예상됩니다.

아울러, 현행 「개인정보 보호법 위반에 대한 과징금 부과기준」에서는 ISMS-P 인증을 받은 경우 개인정보 보호를 위한 노력을 인정하여 최대 50%의 과징금 감경이 가능하도록 규정하고 있으나, 개편된 인증제도 하에서는 사고 발생 시 인증 취소 여부에 따라 과징금 감경 적용이 달라질 수 있으므로 이에 대한 고려가 필요합니다.

나아가, 2025. 9 '개인정보 안전관리 체계 강화 방안'에 따르면 개인정보보호위원회는 2026년 상반기까지 「개인정보 보호법 시행령」 및 「개인정보의 안전성 확보조치 기준」을 개정하여, '주요 개인정보처리시스템을 대상으로 연 1회 모의해킹 실시 및 정보통신망 관리 시스템 등에 대한 취약점 점검 · 보완'을 제도화할 예정입니다.

이와 같이 개인정보 보호를 위한 안전관리 체계에 관한 규제가 강화되는 추세를 감안할 때, 기업들은 정보보호 인력과 예산을 확충하는 등 선제적으로 정보보호 역량을 강화하고, 개인정보 유출 등 사고 대응 체계 또한 보다 강화하여야 할 것입니다.

법무법인(유) 광장 개인정보/DPC 그룹은 개인정보 전문 변호사, 규제기관 출신 및 보안기술 전문가 등 50여명의 전문가들이 포진하여 있으며, 외부 IT/보안 전문가들과 튼튼한 협업 관계를 구축하고 있습니다. 이로써 ISMS · ISMS-P 인증 대응, 정보보호 거버넌스 구축, 개인정보 유출사고 및 침해사고 대응 등 개인정보 보호 및 정보보안 영역 전반에 걸쳐 빠르고 정확한 원스톱 자문 서비스를 제공하고 있습니다.