SHIN&KIM
법무법인(유) 세종

개인정보위, 「예방 중심 개인정보 관리체계 전환 계획」 발표 – 올해 6월부터 위험 기반 실태점검 본격 실시

2026.06.01

개인정보보호위원회(이하 '개인정보위')는 2026년 5월 22일 경제장관회의에서 「예방 중심 개인정보 관리체계 전환 계획」(이하 '본건 전환 계획')을 발표하였습니다. 이는 5월 12일 국무회의에 보고되어 지난 뉴스레터에서 소개해드린 바 있는(링크) 전환 계획을 보다 구체화한 것으로 개인정보 침해·유출 위험을 사전에 식별·관리하는 예방 중심 보호체계로의 전환을 본격 추진하기 위한 것입니다.

최근 인공지능, 플랫폼, 클라우드 기반 서비스의 확산으로 개인정보 처리 규모와 방식이 빠르게 변화함에 따라, 해킹 등 침해 위험이 산업 전반의 리스크로 확대되고 있습니다. 이에 개인정보위는 위험 수준에 비례한 점검·관리를 강화하여 사업자가 필요한 안전조치를 사전에 이행하도록 유도하는 한편, 보호투자 확대, 개인정보 보호 생태계 활성화, 신뢰 문화 조성을 통해 사회 전반의 개인정보 보호 기반을 강화하겠다는 방침입니다.

아래에서 본건 전환 계획의 주요 내용과 시사점을 살펴보겠습니다.

1. 위험 기반 예방관리체계 구축·운영

(위험 기반 실태점검) 개인정보위는 개인정보 처리 규모·민감도·산업별 특성을 고려하여 개인정보 처리 분야를 고·중·저 위험군으로 구분하고, 차등적 점검과 관리를 실시할 계획입니다.

고위험군에 대해서는 점검 분야를 사전에 공개한 뒤 실태점검 후 미흡사항은 시정권고하고 또한 일정 기간 지속적으로 이행여부를 추적 관리하는 등 내부통제 운영 실태를 중점적으로 점검하고 정밀하게 관리할 예정입니다. 이와 같은 고위험군에 대한 점검은 작년 연말 신설된 사전실태점검과에서 중점적으로 추진할 것으로 예상되며, 올해 초부터 진행되고 있는 각종 사전실태점검과 궤를 같이하는 것으로 볼 수 있습니다.

또한, 고위험군에 해당하지 않는 분야에 대해서는 개인정보 영향평가 실시, 개인정보 보호 중심 설계 원칙(Privacy by Design, 이하 "PbD") 적용 등을 유도하고, 자율점검 도구와 컨설팅을 제공하여 개인정보처리자가 자체적으로 기본적인 보호수준을 확보할 수 있도록 지원할 예정입니다.

위험군별 분류 기준과 예방관리 수단은 다음과 같습니다.

<위험 기반 예방관리체계(안)>

구분	분류 기준	예방 관리 수단
고위험	통신/금융/보건·복지 등 고유식별정보·민감정보 등을 대규모(100만 명 이상)로 처리하는 분야	정기·수시 점검, ISMS-P·영향평가 의무화, 보호활동 공개 등
중위험	고위험·저위험에 해당하지 않으나, 체계적인 점검·관리가 필요한 분야	수시·합동점검, 자체 영향평가, PbD 원칙 준수 등
저위험	개인 식별이 어렵거나 영향이 낮은 경우(1만 명 미만 소규모 처리)	자율점검, 안전조치 지원, 구독형 컨설팅 지원 등

더불어 사물인터넷 기기, 에이전트 AI 등 신기술 분야에서의 개인정보 침해 우려사항도 선제적으로 점검 대상에 포함될 것으로 보입니다.

(예방적 보호 제도 개선) 개인정보위는 현행 안전성 확보조치 기준이 개인정보 처리 규모나 위험 수준과 무관하게 일률적으로 적용되어 왔다는 문제의식 아래, 위험분석 결과와 개인정보 처리 흐름·유형을 고려하여 안전조치의 적용 여부 및 수준을 달리 정할 수 있는 방향으로 중장기 개정방안을 마련할 계획입니다. 또한 ISMS-P 인증과 개인정보 영향평가 또한 형식적 법 준수 확인을 넘어, 신기술 위험과 PbD 원칙을 반영하는 상시관리형·위험평가형 제도로 개선할 예정입니다.

2. 자발적 보안·보호 투자 조기 확대 유도

(PbD 원칙 내재화) 개인정보위는 서비스의 기획·설계·개발 단계부터 개인정보 보호를 기본값으로 반영하는 PbD 원칙을 제도화할 계획입니다. 기존에는 IP 카메라, 로봇청소기 등 일부 제품군에 한정하여 PbD 인증제를 운영해 왔으나, 향후 「개인정보 보호법」 개정을 통해 적용 범위를 확대하고, 기획·설계 단계에서 참고할 수 있는 안내서와 우수사례를 보급할 예정입니다. 또한 ISMS-P 인증 등 기존 평가·인증 기준에도 PbD 원칙을 반영함으로써, 개인정보 보호가 사후적 점검사항이 아니라 서비스 전주기에서 고려되어야 할 설계 원칙으로 자리잡도록 할 방침입니다.

(인센티브 재설계 및 책임경영 강화) 기업이 법정 최소기준 준수에 그치지 않고 실질적인 정보보호 투자를 확대하도록 유인하기 위해 인센티브 등 체계를 정비할 예정입니다. 구체적으로 '정보보호 공시'에 추가 보호조치 내역, CPO 내부통제 프로세스 등을 포함하도록 유도하고, 추가적 보호조치가 실효적으로 운영된 사실이 확인되는 경우 과징금 감경 등 인센티브를 부여하는 방안이 검토될 것으로 보입니다. 한편, 중소·영세 사업자의 경미한 위반에 대해서는 기술지원 등을 통한 시정을 전제로 처분을 경감하는 방향도 함께 추진될 예정입니다.

추가적 보호조치의 주요 고려사항 예시는 다음과 같습니다.

<전주기 보호를 위한 추가적 보호조치(예시)>

구분	주요 고려사항 예시
동종업계 대비 우수한 보안투자	IT 대비 보호투자 비중: 금융 9.6%, 정보통신 6% 등
실효적 개인정보 안전관리체계 구축·운영	전담 조직·인력, 영향평가 등 상시위험관리, 신속복구역량

법정 기준을 상회하는 추가적 보호조치	암호화, 추가인증, 취약점 신고·공개제도(CVD·VDP) 등

3. 개인정보 보호 생태계 활성화 및 신뢰 문화 조성

개인정보위는 대량의 개인정보가 집중되는 서비스형 소프트웨어(Software as a Service, SaaS), 클라우드, 전문수탁자 등 개인정보 처리 공급망 전반에 대한 관리를 강화할 계획입니다. 또한 개인정보 유출·오남용을 사전에 방지하기 위한 예방형 개인정보 보호 강화기술(Privacy Enhancing Technologies, PET) 연구개발과 전문인력 양성도 추진할 예정입니다.

이와 함께 아동·청소년 및 취약계층을 대상으로 개인정보 보호 교육을 확대하고, 다크패턴 등 정보주체의 신뢰를 저해할 수 있는 관행을 점검·개선함으로써 개인정보 보호가 일상적 실천 문화로 정착될 수 있도록 지원할 방침입니다.

4. 시사점

- **(위험 기반 점검체계 전환에 따른 사전 대응 필요)** 본건 전환 계획은 개인정보위의 감독 방향이 사후 제재 중심에서 사전 예방 및 위험 기반 관리 중심으로 이동하고 있음을 보여줍니다. 이에 따라 기업으로서는 법상 요구된 최소 기준의 충족 여부만 확인하는 데 그치지 않고, 스스로가 처리하는 개인정보의 규모, 민감도, 처리 방식, 산업 특성 등을 기준으로 개인정보 처리 위험을 선제적으로 진단하고, 그 위험 수준에 부합하는 내부 점검체계를 마련할 필요가 있습니다.
- **(서비스 전 주기 및 공급망 전반에 걸친 개인정보 보호체계 내재화 필요)** 본건 전환 계획은 개인정보 보호가 서비스의 기획·설계·개발·운영 전반에서 일관되게 이루어져야 함을 명확히 하고 있습니다. 이에 따라 기업은 신규 서비스의 기획 단계부터 개인정보 수집 필요성, 처리 목적의 적정성, 정보주체 권리보호 방안 등을 사전에 검토하고, 개발·운영 과정에서도 AI·데이터 활용 확대 등으로 인해 새롭게 발생할 수 있는 위험요인을 지속적으로 점검할 필요가 있습니다. 아울러 공급망 전반에 걸쳐 수탁자 관리·감독 및 침해사고 대응 절차도 함께 정비해 두는 것이 바람직합니다. 또한 위탁자의 수탁자에 대한 관리·감독 책임이 강화되고 있다는 점과 수탁자의 법위반에 따른 제재 사례 또한 증가하고 있다는 점에서 개인정보 처리 업무의 위수탁과 관련한 컴플라이언스 체계도 정비할 필요가 있습니다.
- **(CPO 중심의 내부통제 및 보호조치 입증자료 정비 필요)** 향후 개인정보 보호 활동의 실질적 운영 여부는 점검·평가 및 제재 수준 판단 과정에서 더욱 중요하게 고려될 것으로 보입니다. 특히 CPO 지정 신고제 도입, 정보보호 공시를 통한 보호활동 공개, 추가 보호조치에 대한 인센티브 부여 등이 추진되는 만큼, 기업은 CPO의 권한과 책임, 개인정보 관련 의사결정 절차, 내부통제 프로세스 등을 내부 규정에 명확히 반영할 필요가 있습니다. 나아가 이러한 보호조치가 실제로 운영되고 있음을 입증할 수 있도록 점검 결과, 개선 이행 내역 등 관련 기록을 체계적으로 관리해 두시기를 권해 드립니다.
- **(지속적 동향 모니터링)** 2026년 5월 19일 개정된 개인정보 보호법과 관련한 시행령이 곧 입법예고 될 예정이며, 또한 개인정보위가 지난 5월 12일 보고한 전환 계획에 대해서도 구체화된 사항들이 지속적으로 발표될 것이라는 점에서 향후 마련될 하위법령 및 정책에 대해서도 면밀히 살펴볼 필요가 있다고 할 것입니다.

About Shin & Kim's ICT Group

법무법인(유) 세종 ICT그룹은 ICT 분야의 독보적인 전문성과 인적 네트워크를 보유하고 있으며, 고객들로부터 최근 수년간 가장 높은 평가

를 받고 있습니다. 방송과 통신, 개인정보, 인터넷 IT 분야에서 축적된 역량을 바탕으로 방송·통신·ICT 규제 동향 파악 및 대관, 법제개선·입법컨설팅, 규제영향력 분석과 기업의 전략 수립 등에 대한 종합적인 법률자문을 제공하고 있습니다. AI Compliance, 침해사고 대응 등과 관련하여서도 다양한 업무경험과 전문성을 보유하고 있으므로, 보다 전문적인 내용이나 궁금하신 사항이 있으면 언제든지 연락 주시기 바랍니다.

[English version] PIPC Announces "Transition Plan toward a Prevention-Focused Personal Information Management System" – Risk-Based Inspections to Begin in June

관련구성원

윤종인
고문

02-316-4209
jiyoon@shinkim.com

최광희
고문

02-316-4651
khchoi@shinkim.com

강신욱
대표변호사

02-316-4059
sokang@shinkim.com

안정호
변호사

02-316-2891
jhahn@shinkim.com

윤호상
변호사

02-316-2584
hsyoon@shinkim.com

임새연 (Sally Lim)
외국변호사

02-316-7266
slim@shinkim.com

이다원
변호사

02-316-7962
dwlee@shinkim.com