SHIN&KIM
법무법인(유) 세종

개인정보보호위원회, 「예방 중심 개인정보 관리체계 전환 계획」 발표

2026.05.14

개인정보보호위원회(이하 '개인정보위')는 5월 12일 대통령 주재 국무회의에서 「예방 중심 개인정보 관리체계 전환 계획(이하 '전환 계획')」을 보고하였습니다. 이하에서 전환 계획의 주요 내용 및 시사점을 살펴보겠습니다.

1. 추진 배경

AI·디지털 전환과 플랫폼 경제 확산으로 개인정보 활용의 규모와 범위가 전 분야에서 빠르게 확대되는 가운데, 유출 사고는 대형화되고 있으며 사후 처벌만으로는 피해 회복이 어렵다는 한계점이 드러나고 있습니다. 이에 개인정보위는 이번 전환 계획을 통해 기존의 "사고 후 처벌 중심" 관리 패러다임에서 벗어나, 실질적인 위험 관리와 예방 투자를 유도하는 "사고 전 예방·관리" 체계로의 근본적 전환을 추진하고자 합니다.

2. 주요 내용

개인정보위는 전환 계획의 3대 추진 방향에 따라 다음과 같은 구체적 과제를 제시하였습니다.

(1) 중대·반복 위반 제재 강화

(징벌적 과징금 도입) 고의·중과실로 3년 내 반복 위반을 하거나 1천만 명 이상의 피해가 발생한중대 사고의 경우에는 매출액의 최대 10%까지 과징금을 부과합니다. 이는 현행 최대 3% 수준에서 대폭 상향되는 것으로, 2026년 9월 11일부터 시행되는 개정 개인정보보호법에 따른 것입니다. 한편 시행령 개정을 통해 과징금 산정 기준도 현행 '3년 평균 매출액'에서 '직전 연도 매출액'과 '3년 평균 매출액' 중 높은 금액으로 강화되었는데, 이는 2026년 5월 19일부터 시행됩니다.

구분	현행	개선	시행 예정

징벌적 과징금	매출액의 3%	중대사고·반복 위반 시 매출액의 10%	2026. 9. 11
매출액 산정기준	3년 평균 매출액	직전 연도 매출액과 3년 평균 매출액 중 높은 금액	2026. 5. 19.
조사 강제력	비협조 시 과태료 3천만 원 이하	이행강제금·증거보전명령 추가 도입	법안 발의 ('26. 2.)

(조사 강제력 강화 및 신고포상금 도입) 신속한 조사와 처분을 위해 조사 비협조에 대한 이행강제금 제도를 도입하고, 증거 은닉·폐기 행위에 대한 제재를 강화합니다. 아울러 위반행위 신고를 장려하기 위한 신고포상금 제도도 도입할 계획입니다. 다만, 영세기업의 경미한 위반에 대해서는 시정 기회를 우선 부여하되, 반복 위반 시에는 엄정 대응할 방침입니다.

(2) 자발적 보호투자 확대 및 위험기반 관리체계 구축

(예방투자 인센티브) 형식적인 법령 준수를 넘어 법정 기준을 상회하는 선제적 안전조치, 실효적 안전관리체계 운영, 적극적 보안투자 등 자발적 예방 보호활동에 대해 과징금 감경 등의 인센티브를 부여합니다. 주요 고려사항은 다음과 같습니다.

구분	주요 고려사항 예시
보안 투자	동종업계 대비 우수한 보안 투자 비중 (금융 9.6%, 정보통신 6% 참고)
안전관리체계	전담 조직·인력, 상시 위험관리, 신속복구 역량
추가적 보호조치	암호화, 추가인증, 취약점 신고·공개제도(CVD·VDP) 등

(위험기반 점검체계 구축) 위험 수준에 따라 차등적인 위험기반 관리체계를 구축합니다. 100만 명 이상 개인정보를 처리하는 공공기관·기업 및 클라우드 사업자, 전문수탁사, 시스템 공급사 등 공급망 전반으로 점검을 확대하고, 상조 회사, 고객상담센터, 결혼정보업체, 초·중·고 에듀테크 등도 추가 점검('26~) 대상에 포함합니다.

(개인정보 중심 설계(PbD) 제도화) 서비스가 출시된 이후에는 침해를 인지하거나 방지하기 어렵다는 점을 고려하여, 서비스 기획·설계 단계부터 개인정보 보호를 내재화하는 PbD(Privacy by Design, 개인정보 중심 설계) 원칙을 제도화합니다. 개인정보 영향평가 기준 및 ISMS-P 인증 기준에 PbD 원칙을 반영하고, ISMS-P 인증 체계를 간편-표준-강화 등급으로 세분화하는 한편 인증이 의무화되는 기업의 범위도 확대됩니다.

구분	개선 방향	추진 일정
ISMS-P 인증	인증기준 강화(간편-표준-강화 신설), 상시점검, 공공·민간 주요처리자 의무화	고시 개정('26. 下), 의무화('27. 7.~)
개인정보 영향평가	PbD 원칙 연계, 평가 기준·방법 개선, 민간 확대, 대규모 국외이전 영향평가제 신설	방안 마련('26), 법적 근거 마련('26~)

(경영진 책임 강화 및 전문인력 양성) 오는 9월 11일 시행되는 개정 개인정보 보호법에서는 CEO를 개인정보 보호에 관한 최종적인 책임자로 명시하고 있으며, 일정 규모 이상(100만 명 이상 처리 + 매출액 1,800억 원 이상) 기업은 소정의 자격·경력을 보유한 CPO를 반드시 지

정하도록 하고 있습니다(약 700개 기업이 이에 해당). 또한 CPO 협의회 간 협업을 통한 위협 조기경보 연락체계도 2026년부터 운영하고, 개인정보 보호 전문인력 양성을 위한 대학원 과정을 권역별·지역별로 확대하며, 정책 담당자·개발자·사고 대응 조직 등 직무별 맞춤형 실무 교육 프로그램도 새롭게 설계·운영합니다.

(3) 신속한 피해구제와 회복 지원

(법정 손해배상 활성화) 유출 사고 시 기업·기관이 고의 또는 과실이 없음을 입증하도록 하고 법정 손해배상제도(최대 300만 원)도 도입됩니다. 이는 2026. 9. 11. 시행되는 개정 개인정보보호법에 따른 것입니다.

(국민 권리 강화) 다크패턴처럼 이용자를 속이거나 오인하게 만들어 개인정보 수정·동의 철회·탈퇴를 어렵게 하는 행태를 집중 점검하고, 개인정보 침해신고센터의 기능을 전문 법률상담·피해회복 조력 등 종합지원 체계로 단계적으로 강화합니다.

(불법 유통 엄벌) 민감정보 유출 시 SNS·다크웹 상 불법 유통 여부를 모니터링하여 탐지·삭제하고, 수사기관과 협력하여 불법 유포자 및 이용자를 끝까지 추적·처벌하는 등 엄정 대응합니다.

3. 시사점

- **(징벌적 과징금에 대한 철저한 대비 필요)** 중대·반복 위반 시 매출액의 10%에 달하는 징벌적 과징금은 기업 존립에 영향을 미칠 수 있는 중대한 재무 리스크입니다. 과징금 산정 기준 강화까지 맞물린 만큼, 현행 개인정보 보안체계를 면밀히 점검하고 중대사고나 반복 위반이 발생하지 않도록 내부 점검 체계를 구축하는 것이 중요합니다. 이를 위해 CPO의 권한을 강화하고, 부서 간 협력을 강제할 수 있는 내부 규정 정비 등도 병행할 필요가 있습니다.
- **(보안 투자 인센티브 활용 방안 검토 필요)** 개인정보위가 법정 기준을 상회하는 선제적 보안 투자를 과징금 감경 사유로 적극 반영할 예정인 만큼, 보안 예산·인력·시스템 확충에 대한 전략적 검토가 필요합니다. 선제적 보안 투자가 단순한 비용 지출이 아니라 잠재적 재무 리스크를 최소화할 수 있는 수단이 될 수 있다는 점을 고려하여, 인센티브 요건의 구체적 내용이 확정되는 대로 이에 맞추어 보안투자를 실행하는 등 적시에 대응하는 것이 바람직합니다.
- **(경영진 책임 대응체계 정비 필요)** CEO의 개인정보 보호에 관한 책임이 법에 명시됨에 따라 CEO 차원의 개인정보보호 거버넌스 체계 재정립이 요구됩니다. 또한 소정의 자격·경력을 보유한 CPO의 지정 및 CPO 지정·변경·해제 시 이사회 의결 및 개인정보보호위원회에 대한 신고 등 새롭게 부과되는 절차적 요건에도 유의하여야 합니다.
- **(ISMS-P 인증 및 PbD 도입 준비 필요)** ISMS-P 인증을 받아야 하는 기업의 범위가 확대되고 개인정보 영향평가 기준에 PbD 원칙이 반영될 예정인 만큼, 이에 따른 준비도 차질없이 진행할 필요가 있습니다. 특히 대규모 국외이전 영향평가제 신설은 글로벌 사업을 영위하는 기업에게 추가적인 컴플라이언스 부담으로 작용할 수 있어 유의할 필요가 있습니다.
- **(관련 법령 개정 동향 지속 모니터링 필요)** 이번 전환 계획에서 제시된 과제 중 이행강제금 도입, 신고포상금 제도 도입, 불법 유포자 처벌 강화 등은 현재 법안 발의 단계에 있거나 시행령·고시 개정이 예정되어 있습니다. 각 과제별 후속 입법 동향을 지속적으로 모니터링하면서 기업의 대응체계를 단계적으로 구축해 나갈 필요가 있습니다.

About Shin & Kim's ICT Group 개인정보데이터팀

법무법인(유) 세종은 개인정보 분야에 차별화된 전문성과 인적 네트워크(윤종인 전 개인정보보호위원회 위원장, 김영호 전 행정안전부 차관, 최재유 전 과학기술정보통신부 차관 등)를 보유하고 있으며, 기업들을 위하여 개인정보보호법과 GDPR을 비롯한 국내외 개인정보 규

제, 개인정보 유출사건 대응, 개인정보보호 컴플라이언스 체계 수립 등 개인정보 보호에 관한 전문적인 자문을 제공하고 있습니다. 특히, 최근 발간된 개인정보보호위원회· KCPO의 CPO 핸드북의 감수 및 집필에 참여하는 등 조직 내 개인정보 거버넌스 구축에도 전문성을 보유하고 있습니다. 또한 개인정보 보호법 제2차 개정 및 하위법령 제정, 관련 제도개선에 있어 민간영역에서 주도적인 역할을 수행한 바 있으며, 가명정보, 데이터 활용, ICT 산업 전반에 대한 규제 동향 파악 및 대관, 입법컨설팅, 규제영향력 분석과 기업의 전략 수립 등에 대한 법률자문을 제공하고 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”

관련구성원

윤종인
고문

02-316-4209
jiyoon@shinkim.com

강신욱
대표변호사

02-316-4059
sokang@shinkim.com

안정호
변호사

02-316-2891
jhahn@shinkim.com

노진홍
변호사

02-316-1639
jhnoh@shinkim.com

윤호상
변호사

02-316-2584
hsyoon@shinkim.com

최헌영
변호사

02-316-7247
hyochoi@shinkim.com

유현정
변호사

02-316-1865
hjyoo@shinkim.com