개인정보보호위원회 보도자료 대체불가 대한민국

보도시점 2026.9.10.(목) 11:00 배포 2026.9.10.(목) 9:00

개인정보 유출 사전예방·피해구제 강화를 위한 개인정보 보호법·시행령·고시, 9월 11일부터 시행

- 고의·중과실 등으로 반복·대규모 유출시 엄정 대응, 사전예방 투자에는 인센티브
- 개인정보 보호책임자(CPO) 권한·책임 강화, 이사회 의결·개인정보위 신고 의무
- 개인정보 유출 가능성 통지제 도입, 유출통지 항목 및 대상 확대

국민 일상생활과 밀접한 분야에서 최근 **대규모 개인정보 유출사고**가 연이어 발생하면서 국민들의 불안과 우려가 지속되고 있는 가운데, 개인정보보호위원회(이하 '개인정보위', 위원장 송경희)는 **개인정보 유출사고**를 **사전**에 **예방**하고 국민의 **개인정보 보호**와 **피해구제**를 **강화**하기 위해 제도 개선을 추진하였다. 이를 위해 지난 3월 개정된 「**개인정보 보호법**」(이하 '법')과 위임사항을 구체화한 개정 「**개인정보 보호법 시행령**」(이하 '시행령')이 **9월 11일부터 시행**된다.

지난 3월 개정법에서는 **개인정보 유출**에 **엄정히 대응**하고 **선제적 예방투자**를 촉진하기 위해 ▲**반복적**이거나 **고의·중과실**로 인한 개인정보 유출에 대한 **징벌적 과징금**(전체 매출액 10% 이내) ▲**사전 예방적 개인정보 보호 투자**와 연계한 **과징금 의무 감경제**를 도입하였다.

또한 **개인정보 보호 책임**과 **관리체계**를 **강화**하기 위해 ▲**사업주·대표자**(이하 'CEO')의 **최종책임**을 명시하고 ▲**개인정보 보호책임자**(이하 'CPO')의 **직무권한**을 **강화**(전문인력 관리·예산 확보, 이사회 보고 의무)하였으며 ▲개인정보처리자의 CPO **지정·변경·해제** 시 **이사회 의결** 및 **신고**를 **의무화**하였다.

아울러, 정보주체의 **피해구제**를 강화하기 위해 ▲**개인정보 유출 가능성 통지제**를 신설하고 ▲**유출통지 항목**(분쟁조정 신청, 손해배상 청구 방법도 통지)을 **확대**하였으며, ▲개인정보의 **위조·변조·훼손**(랜섬웨어 등)도 **유출신고·통지 대상**에 **포함**하였다.

법 개정을 통해 **공공·민간** 부문 **중요 개인정보처리자**에 대해 **개인정보 보호**(ISMS-P) **인증**을 **의무화**하는 내용도 포함하였으나, 해당 개정 규정은 ISMS-P 인증 취득을 위한 기업·기관의 예산 확보에 소요되는 기간을 고려하여 **2027년 7월 1일부터 시행**될 예정이다.

※ **ISMS-P 인증 의무화** 관련 **시행령 개정**은 해당 법 규정 시행('27.7.1.) 전까지 **별도 추진**

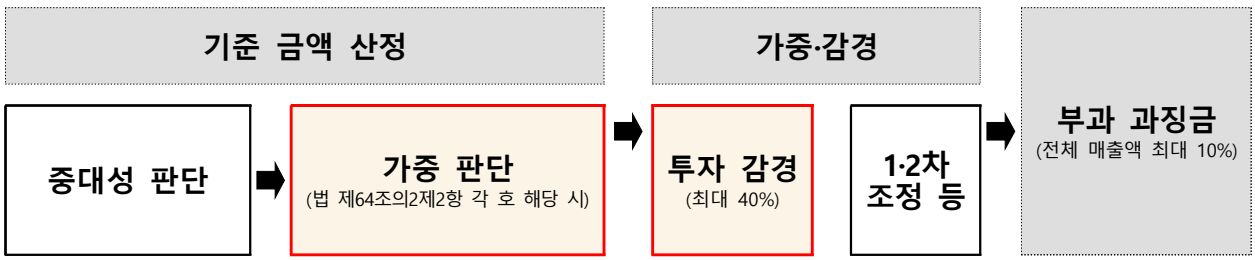
이번 시행령 개정안은 ▲**과징금 부과 기준**과 절차 ▲**선제적 예방투자**에 대한 **과징금 감경기준** ▲**CPO 지정·변경·해제** 시 **이사회 의결** 및 **신고**가 **의무화**되는 **대상 기준**과 **신고 방법** ▲개인정보 **유출 가능성 통지 요건·절차** 등 개정법에서 위임한 사항을 구체화하였다.

개정시행령 및 고시의 **세부 내용**은 다음과 같다.

< ① 반복적·중대한 개인정보 유출에는 엄정 대응하고, 예방 노력은 적극 반영 >

반복적이거나 중대한 개인정보 침해행위에 대해서는 **전체 매출액**의 **최대 10%까지 과징금**을 **부과**할 수 있도록 하는 **과징금 특례**가 시행됨에 따라 과징금 부과·감경 절차와 기준 등 세부사항이 구체화되었다.

< 과징금 산정 흐름도 > ※'26.9.11. 시행



▲**고의·중과실**로 3년 내 위반행위를 **반복**하거나, ▲**고의·중과실**로 **1천만명 이상**의 **대규모 피해**를 발생시킨 경우, ▲**시정명령을 이행하지 않아** 개인정보 **유출사고**가 발생하는 등 개정법 제64조의2제2항 각 호의 어느 하나에 해당하는 경우, **위반행위**의 **내용·정도**와 **경위** 및 **정보주체 피해규모** 등을 **종합 고려**하여 **기준금액**을 **산정**하고, 이후 **가중·감경** 등을 통해 전체 매출액의 10% 이내에서 **부과 과징금**을 **산정**할 수 있도록 **체계적 절차**를 마련하였다.

개인정보 보호를 위해 **사전**에 **적극 투자**하고 **보호체계**를 **강화**한 노력은 **과징금 산정** 과정에서 충분히 **반영**된다. ▲개인정보 보호를 위한 예산·인력·설비·장치 등에 대한 **투자 규모·비율**과 **지속성 및 증가 정도**, ▲CEO·CPO 및 전문인력 등 **개인정보 보호체계**의 **내용**과 **수준**, ▲법상 의무사항 이외의 **안전성 확보조치**에 관한 추가적 노력 등을 고려하여 **과징금 부과 기준금액**의 **40% 범위**에서 **감경**할 수 있도록 하였다.

과징금 감경 시 고려사항 등 제도와 관련한 주요 사항에 대해 「**과징금 투자 감경제도 안내서***」를 발간하여 새롭게 시행되는 제도가 현장에서 제대로 안착될 수 있도록 하였다.

* 개인정보위 누리집(www.pipc.go.kr)>정책·법령>법령정보>안내서에서 내려받기 가능

한편, 기존 **과징금 가중·감경 체계**도 **사전 예방**과 **사후 신속 대응**을 중심으로 변화한다. 우선 **반복 위반**에 대해서는 **가중 비율**을 **상향***하여 **제재**를 **강화**하는 한편, 유출등 **신고·통지**를 **법정기한 내에 이행하지 않고** 정보주체의 **피해 확산 방지 조치도 하지 않는 경우** 과징금을 **가중**(최대 30%)하여 유출 사고 발생 시 **신고 등**을 **하지 않아 오히려 불이익이 적은 구조를 해소**한다.

* **(현행)** (1회)+15% (2회이상)+30% → **(개정)** (1회)+20% (2회)+40% (3회이상)+80%

투자감경 도입과 함께 **ISMS-P 인증, 자율규약 등 개인정보 보호 노력**에 대한 과징금 **감경 비율**을 **조정***하여 **현실화**하는 한편, 높은 수준의 **개인정보 관리 책임성**이 **요구**되는 **주요 공공기관**에 대해서는 **업무 형태·규모**에 따른 **과징금 감경**을 **하지 않도록 명확히 규정**하였다.

* **(현행)** ISMS-P(최대 50%) 자율규약(최대 40%) 보호수준 평가등 (최대 30%)
→ **(개정)** ISMS-P(최대 30%) 자율규약(최대 20%) 보호수준 평가등 (최대 15%)

아울러, 사전 예방 뿐만 아니라 **사후 신속 대응 노력**도 **과징금 감경**에 **반영**된다. **사고 발생**에 대비한 **대응 체계**를 **구축·운영**하고, 사고 시 **조기 탐지, 신속 신고·통지** 및 **피해 확산 방지 조치**를 **이행**하는 등 안전한 개인정보 보호체계로 신속하게 **회복·개선**한 경우 과징금을 감경(최대 40%)한다.

부과 과징금 결정 시 위반행위의 구체적인 내용, 정도와 피해규모 및 영향 등을 고려하여 **추가적으로 감경**(최대 50%)할 수 있도록 하는 등 **비례성**을 **강화**하고, **영세·중소기업** 등의 **경미한 위반**에 대해서는 **기술지원**을 받아 **시정**하는 경우에도 **과징금을 면제**할 수 있도록 하여 **처분 부담**을 **경감**하였다.

< ② 개인정보 보호책임자(CPO)의 권한·책임과 독립성 강화 >

법 개정으로 CPO를 **지정·변경·해제**할 때 **이사회 의결**을 거치고 개인정보위에 **신고**해야 하는 의무가 신설되어, **의무**가 부여되는 **대상 기준**을 시행령 개정을 통해 구체화하였다.

주요 개인정보처리자를 중심으로 CPO의 권한과 책임을 높이기 위해, 이사회 의결·신고 **의무 대상**은 현행법상 **전문 CPO 지정 의무 대상**과 동일*하게 하였다.

* ▲연 매출액 또는 수입이 **1,800억 원을 초과**하면서 **5만 명 이상**의 **민감정보·고유식별정보** 또는 **100만 명 이상**의 개인정보를 처리하는 자, **▲재학생 수 2만 명 이상**인 **대학**, **▲상급 종합병원**, **▲공공시스템운영기관**(시행령 제30조의2제1항에 따른 주요 공공시스템을 운영하는 기관)

신고 대상이 되는 개인정보처리자는 법 시행 이후 **CPO를 지정·변경·해제**하려는 경우 **이사회 의결**을 거치고 **신고 사유**가 **발생한 날**로부터 **6개월 이내**에 개인정보위에 **신고서**를 **제출**하여야 한다. **법 시행 전**에 **지정되어 있는** CPO에 대해서는 별도의 이사회 의결을 거치지 않아도 되며 **법 시행일**(9.11.)부터 **6개월 이내** 개인정보위에 **신고**하여야 한다. 다만, 경영상의 이유로 이사회 소집이 어려운 경우 등 **부득이한 사유**가 있다고 개인정보위가 인정하는 경우에는 개인정보처리자의 요청에 따라 **최대 1년**까지 **신고 기간을 연장**할 수 있다.

또한, 기존 「**CPO 경력 인정에 관한 고시**」를 개정하여 **CPO 지정·변경·해제 신고서**를 **마련**하고 신고 절차를 구체화하였다. **CPO 지정 신고 방법**은 "**개인정보 포털**(www.privacy.go.kr)"에 접속 후 「기업·공공 서비스」 메뉴의 「CPO 신고」를 선택하여 **신고 항목***을 **입력**하고 **증빙자료**를 **첨부**하는 등 신고 절차를 진행하면 된다.

* **(신고인)** 상호명(법인명), 사업자등록번호(법인등록번호), 소재지, 대표자, 전화번호
(CPO) 성명, 전화번호, 전자우편주소, 직책/직급, 업무경력 등

개인정보위는 신규 CPO 제도 도입에 따른 **대상기관**의 **부담**을 **완화**하고 제도의 안정적 정착을 도모하기 위해 **2027년 12월 31일**까지 **계도기간**을 **운영**할 예정이며, 계도기간 중에는 **▲CPO 미지정 ▲CPO 자격요건 미비 ▲이사회 의결 의무 위반 ▲신고 해태** 등 법령 위반에 대해 **과태료**가 **부과되지 않는다.**

아울러, 제도 시행 초기 **현장 적용성**을 **강화**하고 **대상기관**이 **의무를 준수**할 수 있도록 CPO **제도 전반**에 대한 **설명**과 신고 방법, **주요 FAQ**를 담은 「**CPO 지정·신고 실무 매뉴얼***」을 마련하여 공개하는 한편, 한국CPO협의회** 등 유관 협회와 협업하여 **현장 안내**를 **지속**할 계획이다.

* 개인정보위 누리집(www.pipc.go.kr)>정책·법령>법령정보>안내서에서 내려받기 가능
** 한국CPO협의회 누리집(www.k-cpo.org)

< ③ 개인정보 유출 가능성 단계부터 국민에게 신속히 통지 >

개인정보 유출등으로 인한 국민의 피해를 최소화하기 위해 유출 사실이 최종적으로 확인되기 전이라도 **객관적으로 유출 가능성**이 높다고 합리적으로 판단되는 경우에는 **정보주체**에게 이를 **통지**하도록 하는 유출 가능성 통지제가 도입됨에 따라, 요건·절차·항목 등이 구체적으로 마련되었다.

▲개인정보처리시스템, 개인정보취급자가 이용하는 기기에 **불법적인 접근**이 발생하여 개인정보 유출등이 의심되나 **정보주체**를 **특정**하기 **곤란한 경우**, ▲개인정보가 **불법적**으로 **거래**되는 등 일부 개인정보의 **유출등**이 **확인**되어 **다른 정보주체**의 **개인정보**도 **유출등 가능성**이 있다고 인정되는 경우 해당 사실을 **알게 된 때**부터 **72시간 이내**에 **정보주체**에게 **통지***하여야 한다. 이 때 통지 항목**은 유출등 통지에 준하는 수준으로 알려야 한다.

* 다만 부득이한 사유로 기한 내 통지하기 곤란한 경우 해당 사유 해소 후 즉시 통지, 유출등 가능성 통지 기한 내 실제 유출등이 확인된 경우 유출등 통지로 갈음하고, 유출되지 않았음이 확인된 경우에는 정보주체 혼란·불안 해소를 위해 정정 통지 필요

** 1. 개인정보 항목 2. 의심시점·경위 3. 피해최소화 방법 4. 피해구제절차 5. 피해신고 연락처 6. 유출등 확정시 추가통지하겠다는 사실 등

아울러, 유출등 사고 시 대응 및 국민의 피해구제가 보다 신속히 이루어질 수 있도록 법 개정사항을 반영하고 구체적 기준 및 사례 안내 등을 보강하여 「**개인정보 유출등 대응 안내서***」를 개정하였다.

* 개인정보위 누리집(www.pipc.go.kr)>정책·법령>법령정보>안내서에서 내려받기 가능

송경희 개인정보위 위원장은 "이번 **개정법령 시행**을 계기로 **사전예방 중심**의 **개인정보 보호**, **강화된 안전관리 체계**가 **확립**되고, 개인정보 보호를 위한 투자를 '비용'이 아니라 고객 신뢰 확보와 기업 이익 확대를 위한 '**선제적 투자**'로 **인식**이 **전환**될 것으로 기대한다"고 밝혔다.

개정법령 시행을 통해 개인정보 유출등 침해에 대한 **기업·기관**의 **책임**이 **강화**되고, 국민들은 **개인정보 유출 위험**을 보다 **신속하게 안내**받을 수 있게 된다. 아울러 개인정보 보호 **사전예방 투자**와 연계한 **과징금 감경제 도입**, **CEO·CPO 책임 강화**를 통해 개인정보처리자의 상시적인 **개인정보 안전관리 체계**가 정착될 수 있을 것으로 기대된다.

개인정보위는 **새롭게 시행되는 제도**가 현장에서 **안정적**으로 **운영**되고 기업·기관과 국민들이 쉽게 이해할 수 있도록 **지속적**으로 **안내**할 계획이다.

담당 부서 <총괄>	개인정보보호위원회 개인정보보호정책과	책임자	과 장	최윤정 (02-2100-3051)
		담당자	사무관	김지영 (02-2100-3057)
<유출통지> < 과징금 > <투자감경>	조사총괄과	책임자	과 장	강대현 (02-2100-3101)
		담당자	사무관	장수용 (02-2100-3102)
			사무관	전창민 (02-2100-3161)
			주무관	김아림 (02-2100-3163)
			사무관	송진헌 (02-2100-3110)
<CPO 제도>	자율보호정책과	책임자	과 장	황지은 (02-2100-3081)
		담당자	사무관	공수진 (02-2100-3082)

참고1 투자감경 안내서 개요

□ 총괄

○ 위반행위가 발생하기 전 **3개 사업연도 범위내**에서 다음 각 호의 요건을 종합적으로 고려(고의 또는 중과실에 의한 위반행위는 제외)

※ 위원회가 상당하다고 인정하는 경우에는 위반행위가 있었던 사업연도에 조치한 사항 고려 가능(예 : 사업을 개시한지 1년 미만된 기업 등)

- 감경 요건 고려 시, **안내서에 제시한 예시 이외**에도 각 요건을 충족하기 위해 노력하여 우수하다고 인정되는 경우 **감경 요소로 고려 가능**

< 과징금 산정 절차 >

투자 감경(추가) ⇒ 1차 조정 ⇒ 2차 조정 ⇒ 부과 과징금 결정

1 예산 · 인력 · 설비 · 장치 등의 투자 규모, 비율, 지속성 및 증가 정도

○ ①개인정보보호 관련 **예산편성 및 집행정도**, ②일회성 투자가 아닌 **지속적 투자 여부**, ③투자의 증가정도, ④신규 투자 정도 등 고려

※ (관련 지표 예시) IT 투자액 대비 개인정보보호 투자 예산 비율, 개인정보보호 투자 금액 증가율 및 집행 내역, 매출액 대비 개인정보 보호 투자 규모 등

※ 업종별 특성 등을 고려한 비교는 향후 공시제도 개선 등을 토대로 검토 예정

2 CEO · CPO 및 조직 · 인력 등 개인정보 보호체계 운영 수준의 우수성

구분	판단 기준	세부 고려사항(주요 예시)
CEO	CEO의 관심도·실천의지 등	▶ 개인정보 보호를 위한 **실효적 관리체계의 구축** 여부
CPO	업무 수행도·전문성·실질적 권한 부여 여부 등	▶ CPO **업무 수행의 충실성** ▶ CPO가 법적 자격 요건 이외 **추가적 자격 요건**을 갖추고 있는지 ▶ 기업 내 **최상위 의사결정기구에 참여**하고 있는지
조직·인력	관련 체계의 성숙도	▶ 개인정보 전담·담당 인력에 대한 **전문성 강화 및 처우 개선**에 대한 노력

3 법상 의무사항 이외의 안전성 확보조치 수준의 우수성

○ 기존 안전성 확보조치 기준에서 정하고 있는 **안전조치를 기준 이상으로 적용한 경우** 등을 감경 요소로 고려

< 세부 고려사항 >

① **내부관리계획 이행 실태 지속 점검** - (예시) 상시적 위험관리체계 구축	② **접근 권한의 체계적 관리** - (예시) 계정 및 접근권한 통합 관리
③ **안전한 인증수단 확대 적용** - (예시) 안전한 인증수단 및 접속수단 동시 적용	④ **공격표면 관리 및 취약점 점검·조치** - (예시) CVD·VDP 상시 참여
⑤ **암호화 대상 개인정보 항목 확대 적용** - (예시) 법적 대상 이외 추가 암호화	⑥ **암호키 유출방지 기술 적용** - (예시) 하드웨어 보안모듈 적용
⑦ **로그 관리 강화** - (예시) 로그기록을 실시간 통합 관리	⑧ **S/W 공급망 및 보안패치 관리** - (예시) SBOM 기록하고 현행화

참고2 개인정보 보호책임자(CPO) 제도 개요

□ 추진 배경

○ 국민 신뢰 기반의 **데이터 거버넌스** 조성에 **개인정보 보호책임자**(CPO)가 **핵심역할을 수행**하도록 보호법령 개정하여 **전문 CPO 제도*** **시행**('24.3.15.)

- CPO의 **전문성 강화·독립성 보장**을 위한 **제반여건을 마련**하여, **개인정보보호 전담인력**으로서의 **실질적 역할 강화** 및 **위상 제고**

* 개인정보처리자의 매출액과 개인정보의 보유 규모를 고려, 전문자격을 갖춘 CPO 지정 의무화 및 CPO가 정기적으로 대표자 또는 이사회에 직접 보고하는 체계 마련 등

□ 주요 내용

○ 개인정보처리자의 유형·특성을 고려 CPO 직위요건 규정

공공기관	① 중앙행정기관/국가기관 : 고위공무원/4급이상 공무원, 시·도 : 3급 이상 공무원 등 ② 각급 학교 : 해당학교의 행정사무를 총괄하는 사람 등 ③ 그 외 공공기관 : 개인정보 처리 관련 업무를 담당하는 부서의 장
민간기업	① 사업주 또는 대표자 ② 임원 ③ 임원이 없는 경우 개인정보 처리 업무 담당 부서장

○ **중요 개인정보처리자 대상 CPO 자격요건 도입 시행**('24.3.15) 및 CPO 지정·변경·해제 시 **이사회 의결** 및 **개인정보위 신고** 의무화('26.9.11.)

적용대상	① 연 매출액 또는 수입이 **1,800억원**을 **초과**하는 자로서, **100만명 이상 개인정보** 또는 **5만명 이상 민감·고유식별정보**를 처리하는 개인정보처리자 ② 재학생 수 **2만 명 이상**인 **대학**(대학원 재학생 수 포함) ③ 대규모 민감정보(건강정보)를 처리하는 **상급종합병원** ④ **공공시스템운영기관**
자격요건	개인정보보호·정보보호·정보기술 경력을 합하여 **총 4년 이상** 보유(**개인정보 경력 2년** 필수)

○ CPO의 독립성을 보장하기 위한 **개인정보처리자**의 **준수 의무*** 규정

* CPO의 개인정보 처리 관련 정보 접근보장, 정기적으로 대표자 또는 이사회에 직접 보고 가능 체계 구축, 업무수행에 적합한 조직체계 마련, 인적·물적 자원 제공 등

○ **CPO 협의회 설립으로 CPO 간 교류협력 강화**

※ 개인정보보호법 제31조에 따라 개인정보처리자는 CPO협의회를 구성·운영할 수 있으며, 개인정보위는 CPO협의회 활동 지원 가능

참고3 유출통지·신고 제도 법 개정 사항

□ 개정 배경

○ 현행 법은 **통지 의무**를 '유출 등이 되었음을 **알았을 때**'로 **한정**하고, **통지·신고 대상**이 되는 **사고 유형**의 **범위**도 **제한적**이어서,

- 대규모 유출 **가능성**이 있는 사고 초기 단계나 **위조·변조·훼손** 등 다양한 형태의 사고에 대해 **정보주체**의 **즉각적 대응 및 대비**가 어려웠음

□ 개정 내용

○ 대규모 피해를 초래하는 사고 발생 초기부터 정보주체가 신속하게 대응할 수 있도록 **유출 가능성**이 있는 경우도 **통지 의무화**

○ 아울러 '**위조·변조·훼손**'도 **통지·신고 대상**에 포함, **통지항목 확대**, 유출 시 개인정보 삭제·회수 등 **피해 확산 방지 조치 강화**

현 행		개 선
대상	분실·도난·**유출**	**위조·변조·훼손 추가**(랜섬웨어 등)
기준	유출 등이 되었음을 **알게 되었을 때**로 한정	**유출 등의 가능성이 있음을 알게 된 때**
항목	항목·시점·경위, 피해 최소화 방법, 피해구제 절차 등	**법적 피해구제 절차 추가** (손해배상 청구, 분쟁조정 등) 등
확산 방지	피해 최소화 대책 마련·조치	**개인정보의 회수·삭제 등** 구체화