

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 유출사고가 연이어 발생하면서 국민들의 불안과 우려가 지속되고 있는 가운데, 개인정보 보호위원회(이하 ‘개인정보위’, 위원장 송경희)는 개인정보 유출사고를 사전에 예방하고 국민의 개인정보 보호와 피해구제를 강화하기 위해 제도 개선을 추진하였다. 이를 위해 지난 3월 개정된 「개인정보 보호법」(이하 ‘법’)과 위임 사항을 구체화한 개정 「개인정보 보호법 시행령」(이하 ‘시행령’)이 9월 11일부터 시행된다.

지난 3월 개정법에서는 개인정보 유출에 엄정히 대응하고 선제적 예방 투자를 촉진하기 위해 ▲반복적이거나 고의·중과실로 인한 개인정보 유출에 대한 징벌적 과징금(전체 매출액 10% 이내) ▲사전 예방적 개인정보 보호 투자와 연계한 과징금 의무 감경제를 도입하였다.

또한 개인정보 보호 책임과 관리체계를 강화하기 위해 ▲사업주·대표자(이하 ‘CEO’)의 최종책임을 명시하고 ▲개인정보 보호책임자(이하 ‘CPO’)의 직무 권한을 강화(전문인력 관리·예산 확보, 이사회 보고 의무)하였으며 ▲개인정보처리자의 CPO 지정·변경·해제 시 이사회 의결 및 신고를 의무화하였다.

아울러, 정보주체의 피해구제를 강화하기 위해 ▲개인정보 유출 가능성 통지제를 신설하고 ▲유출통지 항목(분쟁조정 신청, 손해배상 청구 방법도 통지)을 확대하였으며, ▲개인정보의 위조·변조·훼손(랜섬웨어 등)도 유출신고·통지 대상에 포함하였다.

법 개정을 통해 공공·민간 부문 중요 개인정보처리자에 대해 개인정보 보호(ISMS-P) 인증을 의무화하는 내용도 포함하였으나, 해당 개정 규정은 ISMS-P 인증 취득을 위한 기업·기관의 예산 확보에 소요되는 기간을 고려하여 2027년 7월 1일부터 시행될 예정이다.

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

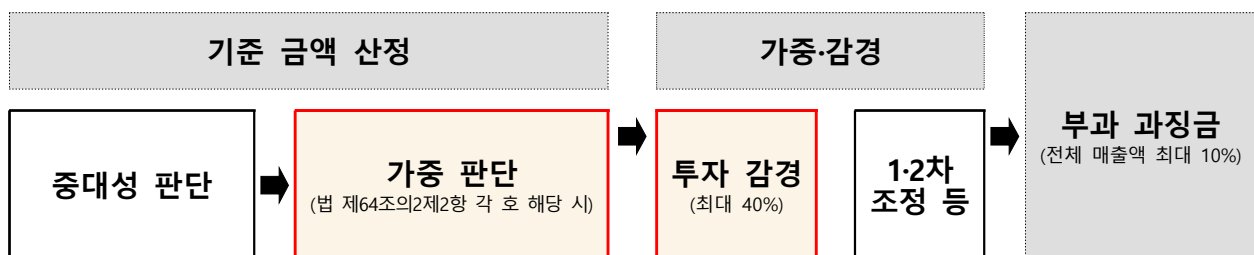
이번 시행령 개정안은 ▲과징금 부과 기준과 절차 ▲선제적 예방투자에 대한 과징금 감경기준 ▲CPO 지정·변경·해제 시 이사회 의결 및 신고가 의무화되는 대상 기준과 신고 방법 ▲개인정보 유출 가능성 통지 요건·절차 등 개정법에서 위임한 사항을 구체화하였다.

개정시행령 및 고시의 세부 내용은 다음과 같다.

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

반복적이거나 중대한 개인정보 침해행위에 대해서는 전체 매출액의 최대 10%까지 과징금을 부과할 수 있도록 하는 과징금 특례가 시행됨에 따라 과징금 부과·감경 절차와 기준 등 세부사항이 구체화되었다.

< 과징금 산정 흐름도 > ※ '26.9.11. 시행



▲ 고의·중과실로 3년 내 위반행위를 반복하거나, ▲ 고의·중과실로 1천만명 이상의 대규모 피해를 발생시킨 경우, ▲ 시정명령을 이행하지 않아 개인정보 유출사고가 발생하는 등 개정법 제64조의2제2항 각 호의 어느 하나에 해당하는 경우, 위반행위의 내용·정도와 경위 및 정보주체 피해규모 등을 종합 고려하여 기준금액을 산정하고, 이후 가중·감경 등을 통해 전체 매출액의 10% 이내에서 부과 과징금을 산정할 수 있도록 체계적 절차를 마련하였다.

개인정보 보호를 위해 사전에 적극 투자하고 보호체계를 강화한 노력은 과징금 산정 과정에서 충분히 반영된다. ▲개인정보 보호를 위한 예산·인력·설비·장치 등에 대한 투자 규모·비율과 지속성 및 증가 정도, ▲CEO·CPO 및 전문인력 등 개인정보 보호체계의 내용과 수준, ▲법상 의무사항 이외의 안전성 확보조치에 관한 추가적 노력 등을 고려하여 과징금 부과 기준금액의 40% 범위에서 감경할 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 체계도 사전 예방과 사후 신속 대응을 중심으로 변화한다. 우선 반복 위반에 대해서는 가중 비율을 상향*하여 제재를 강화하는 한편, 유출등 신고·통지를 법정기한 내에 이행하지 않고 정보주체의 피해 확산 방지 조치도 하지 않는 경우 과징금을 가중(최대 30%)하여 유출 사고 발생 시 신고 등을 하지 않아 오히려 불이익이 적은 구조를 해소한다.

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

투자감경 도입과 함께 ISMS-P 인증, 자율규약 등 개인정보 보호 노력에 대한 과징금 감경 비율을 조정*하여 현실화하는 한편, 높은 수준의 개인정보 관리 책임성이 요구되는 주요 공공기관에 대해서는 업무 형태·규모에 따른 과징금 감경을 하지 않도록 명확히 규정하였다.

* **(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 노력도 과징금 감경에 반영된다. 사고 발생에 대비한 대응 체계를 구축·운영하고, 사고 시 조기 탐지, 신속 신고·통지 및 피해 확산 방지 조치를 이행하는 등 안전한 개인정보 보호체계로 신속하게 회복·개선한 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 비례성을 강화하고, 영세·중소기업 등의 경미한 위반에 대해서는 기술지원을 받아 시정하는 경우에도 과징금을 면제할 수 있도록 하여 처분 부담을 경감하였다.

< ② 개인정보 보호책임자(CPO)의 권한·책임과 독립성 강화 >

법 개정으로 CPO를 지정·변경·해제할 때 이사회 의결을 거치고 개인정보 위에 신고해야 하는 의무가 신설되어, 의무가 부여되는 대상 기준을 시행령 개정을 통해 구체화하였다.

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

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

신고 대상이 되는 개인정보처리자는 법 시행 이후 CPO를 지정·변경·해제하려는 경우 이사회 의결을 거치고 신고 사유가 발생한 날로부터 6개월 이내에 개인정보위에 신고서를 제출하여야 한다. 법 시행 전에 지정되어 있는 CPO에 대해서는 별도의 이사회 의결을 거치지 않아도 되며 법 시행일(9.11.)부터 6개월 이내 개인정보위에 신고하여야 한다. 다만, 경영상의 이유로 이사회 소집이 어려운 경우 등 부득이한 사유가 있다고 개인정보위가 인정하는 경우에는 개인정보처리자의 요청에 따라 최대 1년까지 신고기간을 연장할 수 있다.

또한, 기존 「CPO 경력 인정에 관한 고시」를 개정하여 CPO 지정·변경·해제 신고서를 마련하고 신고 절차를 구체화하였다. CPO 지정 신고 방법은 “개인정보 포털(www.privacy.go.kr)”에 접속 후 「기업·공공 서비스」 메뉴의 「CPO 신고」를 선택하여 신고 항목*을 입력하고 증빙자료를 첨부하는 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 대상기관의 부담을 완화하고 제도의 안정적 정착을 도모하기 위해 2027년 12월 31일까지 계도기간을 운영할 예정이며, 계도기간 중에는 ▲CPO 미지정 ▲CPO 자격요건 미비 ▲이사회 의결 의무 위반 ▲신고 해태 등 법령 위반에 대해 과태료가 부과되지 않는다.

아울러, 제도 시행 초기 현장 적용성을 강화하고 대상기관이 의무를 준수할 수 있도록 CPO 제도 전반에 대한 설명과 신고 방법, 주요 FAQ를 담은 「CPO 지정·신고 실무 매뉴얼*」을 마련하여 공개하는 한편, 한국CPO협회** 등 유관 협회와 협업하여 현장 안내를 지속할 계획이다.

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

** 한국CPO협회 누리집(www.kcpo.or.kr)

< ③ 개인정보 유출 가능성 단계부터 국민에게 신속히 통지 >

개인정보 유출등으로 인한 국민의 피해를 최소화하기 위해 유출 사실이 최종적으로 확인되기 전이라도 객관적으로 유출 가능성이 높다고 합리적으로 판단되는 경우에는 정보주체에게 이를 통지하도록 하는 유출 가능성 통지제가 도입됨에 따라, 요건·절차·항목 등이 구체적으로 마련되었다.

▲개인정보처리시스템, 개인정보취급자가 이용하는 기기에 불법적인 접근이 발생하여 개인정보 유출등이 의심되거나 정보주체를 특정하기 곤란한 경우, ▲개인정보가 불법적으로 거래되는 등 일부 개인정보의 유출등이 확인되어 다른 정보주체의 개인정보도 유출등 가능성이 있다고 인정되는 경우 해당 사실을 알게 된 때부터 72시간 이내에 정보주체에게 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 시행을 계기로 사전예방 중심의 개인정보 보호, 강화된 안전관리 체계가 확립되고, 개인정보 보호를 위한 투자를 ‘비용’이 아니라 고객 신뢰 확보와 기업 이익 확대를 위한 ‘선제적 투자’로 인식이 전환될 것으로 기대한다”고 밝혔다.

개정법령 시행을 통해 개인정보 유출등 침해에 대한 기업·기관의 책임이 강화되고, 국민들은 개인정보 유출 위험을 보다 신속하게 안내받을 수 있게 된다. 아울러 개인정보 보호 사전예방 투자와 연계한 과징금 감경제 도입, CEO·CPO 책임 강화를 통해 개인정보처리자의 상시적인 개인정보 안전관리 체계가 정착될 수 있을 것으로 기대된다.

개인정보위는 새롭게 시행되는 제도가 현장에서 안정적으로 운영되고 기업·기관과 국민들이 쉽게 이해할 수 있도록 지속적으로 안내할 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	송진현 (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 범위내에서 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 이외에도 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 요건을 갖추고 있는지 ▶ 기업 내 최상위 의사결정기구에 참여하고 있는지
조직·인력	관련 체계의 성숙도	▶ 개인정보 전담·담당 인력에 대한 전문성 강화 및 처우 개선에 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

□ 추진 배경

- 국민 신뢰 기반의 데이터 거버넌스 조성에 개인정보 보호책임자(CPO)가 핵심역할을 수행하도록 보호법령 개정하여 전문 CPO 제도* 시행(“24.3.15.)

- CPO의 전문성 강화 · 독립성 보장을 위한 제반여건을 마련하여, 개인정보보호 전담인력으로서의 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 1,800억원을 초과하는 자로서, 100만명 이상 개인정보 또는 5만명 이상 민감·고유식별정보를 처리하는 개인정보처리자 ② 재학생 수 2만 명 이상인 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 개인정보처리자의 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

□ 개정 배경

- 현행 법은 통지 의무를 ‘유출 등이 되었음을 알았을 때’로 한정하고, 통지·신고 대상이 되는 사고 유형의 범위도 제한적이어서,
 - 대규모 유출 가능성이 있는 사고 초기 단계나 위조·변조·훼손 등 다양한 형태의 사고에 대해 정보주체의 즉각적 대응 및 대비가 어려웠음

□ 개정 내용

- 대규모 피해를 초래하는 사고 발생 초기부터 정보주체가 신속하게 대응할 수 있도록 유출 가능성이 있는 경우도 통지 의무화
- 아울러 ‘위조·변조·훼손’도 통지·신고 대상에 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 때로 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