

발 간 등 록 번 호

11-1790365-100050-01



과징금 투자 감경제도 안내서

2026. 9.



개인정보보호위원회

personal Information Protection Commission

발 간 등 록 번 호
11-1790365-100050-01

과징금 투자 감경제도 안내서

2026. 9.



개인정보보호위원회

personal Information Protection Commission

과징금 투자 감경제도 안내서

안내 사항

발간 목적

본 안내서는 「개인정보 보호법」 개정에 따라 시행되는 과징금 투자 감경제도의 주요 사항을 안내합니다.

재검토 기한

안내서의 최신성을 유지하기 위해 발간일(2026년 09월)을 기준으로 3년마다(매 3년이 되는 해의 1월 1일 전까지를 말함) 보완 및 개선 등의 조치를 위해 그 타당성을 검토할 예정입니다.

저작권 표시

본 안내서 내용의 무단전재를 금하며, 가공·인용할 때는 출처를 밝혀 주시기 바랍니다.

* 출처 : 개인정보보호위원회, 「과징금 투자 감경제도 안내서」 2026.09.

문의처

본 안내서 내용 관련 문의는 개인정보보호위원회 조사총괄과(☎02-2100-3110)로 문의주시기 바랍니다.

관계법령

「개인정보 보호법」 제64조의2(과징금의 부과)

※ 법령 최신 자료는 국가법령정보센터(www.law.go.kr), 개인정보 보호 안내서 최신 자료는 개인정보보호위원회 누리집*, 개인정보 포털**을 참고

* 개인정보보호위원회 누리집(www.pipc.go.kr) : 법령 > 법령정보 > 안내서

** 개인정보 포털(www.privacy.go.kr) : 자료 > 자료보기 > 안내서

C O N T E N T S

I

개요 6

- 1. 개정 개요 6
- 2. 개정 법령 6
- 3. 주요 내용 7

II

요건별 세부 기준 8

- 1. 개인정보 보호를 위한 투자 규모 및 지속성 8
- 2. 개인정보 보호체계의 우수성 12
- 3. 안전조치 확보를 위한 추가적 노력 17



I

개요

I 개요

1 개정 개요

- 최근 대규모 개인정보 유출사고가 반복적으로 일어남에 따라 기존의 과징금 처분 등 사후적 제재 이외의 **사전예방의 중요성이 증대**
- 이에, 기업의 실질적인 예방투자를 장려하기 위해 **예산·인력·설비·장치 등 개인정보 보호에 선제적으로 투자하고 운영한 노력이 인정되면 과징금을 감경**하도록 법률 근거를 신설하였음('26.3.10.)

2 개정 법령

법률	제64조의2(과징금의 부과) ⑥ 보호위원회는 개인정보 보호를 위하여 예산·인력·설비·장치 등을 투자하고 운영하는 등 대통령령으로 정하는 사유가 있는 경우에는 제1항 및 제2항에 따른 과징금을 감경한다. 다만, 개인정보처리자의 고의 또는 중대한 과실로 위반행위를 한 경우는 제외한다.
시행령	제60조의2(과징금의 산정기준 등) ⑤ 법 제64조의2제6항 본문에서 “개인정보 보호를 위하여 예산·인력·설비·장치 등을 투자하고 운영하는 등 대통령령으로 정하는 사유가 있는 경우”란 개인정보 보호를 위하여 예산·인력·설비·장치 등을 투자하고 운영하는 경우로서 다음 각 호의 사항을 고려하여 보호위원회가 정하여 고시하는 기준을 충족하는 경우를 말한다. 1. 개인정보 보호를 위하여 예산·인력·설비·장치 등에 투자한 규모·비율 및 그 투자의 지속성 2. 법 제30조의3에 따른 사업주 또는 대표자의 책임 이행 정도 3. 개인정보 보호책임자의 역할, 조직 및 인력 구성 등 개인정보 보호 체계 운영 내용 및 수준 4. 그 밖에 개인정보 안전성 확보 조치에 관한 추가적인 노력 [별표 1의5] 나. 투자 감경 법 제64조의2제6항에 따라 가목에 따른 기준금액의 100분의 40의 범위에서 제60조의2 제5항의 사유를 고려하여 보호위원회가 정하여 고시하는 기준에 따라 감경한다.
고시	제8조의3(투자감경) ① 다음 각 호의 사항을 종합적으로 고려하여 기준금액의 100분의 40 이하에 해당하는 금액을 감경한다. 다만, 법 제64조의2제6항 단서에 해당하는 경우는 제외한다. 1. 개인정보 보호를 위하여 예산·인력·설비·장치 등에 투자한 규모·비율, 그 투자의 지속성, 증가 정도 등이 우수한 경우 2. 법 제30조의3에 따른 사업주 또는 대표자의 책임 이행 정도, 개인정보 보호책임자의 지정·권한 책임 이행 및 업무수행 수준, 인력 구성·운영 등 개인정보 보호 체계의 운영 수준이 우수한 경우

3. 법상 의무사항 이외의 강화된 보호기술의 적용 등 **안전성 확보조치 수준이나 노력 등이 우수한 경우**
- ② 제1항에 따라 금액을 감경할 때에는 **위반행위가 있었던 사업연도의 직전 3개 사업연도 범위 내에서 조치한 사항**을 고려하되, **위원회가 상당하다고 인정하는 경우에는 위반행위가 있었던 사업연도에 조치한 사항을 고려할 수 있다.**

3 주요 내용

가. 요건

■ **위반행위가 발생하기 전 3개 사업연도 범위내에서** 다음 각 호의 요건을 종합적으로 고려

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

- ① 개인정보 보호를 위하여 예산·인력·설비·장치 등에 **투자한 규모·비율 및 지속성**
- ② 사업주 또는 대표자의 책임 이행 정도, 개인정보 보호책임자의 역할, 조직 및 인력 구성 등 **개인 정보 보호 체계 운영 내용 및 수준**
- ③ 개인정보 **안전성 확보 조치 강화**를 위한 추가 노력

■ 단, 제재의 실효성이 약화되지 않도록 하기 위해 **개인정보처리자의 고의 또는 중과실에 의한 위반행위**에 대해서는 감경 제외

■ 감경 요건 고려 시, 개인정보처리자의 규모 등을 고려하여 판단하며 안내서에 제시한 예시 이외에도 각 요건을 충족하기 위해 노력하여 우수하다고 인정되는 경우 감경 요소로 고려 가능

나. 감경 정도

■ 경제적 인센티브를 통한 사전 예방 체계 구축이 확산될 수 있도록 **최대 40% 수준의 감경을 적용**

다. 산정 절차



II 요건별 세부 기준

1 개인정보 보호를 위한 투자 규모 및 지속성

① 주요 내용

- 위반행위가 있었던 사업연도(‘해당 사업연도’)의 직전 3개 사업연도 범위내에서 예산·인력·설비·장치 등에 대한 투자 규모·투자의 지속성 및 증가 정도 등을 고려

② 세부 고려 사항(예시)

- 개인정보 보호를 위해 예산을 적극적으로 편성하고 실제 집행하고 있는지
- 예산·인력·설비·장치 등에 대해 일회성 투자가 아닌 지속적인 투자가 이루어지고 있는지
- 예산·인력·설비·장치 등에 대한 투자의 증가 여부 및 증가 정도
- 개인정보 보호를 위한 적극적이고 새로운 투자 이행 정도

※ 기존 투자 내역에 대한 지속적 운영노력을 고려사항에서 배제하는 것은 아님

< 관련 사례 >

▶ 개인정보 보호 예산* 및 실제 집행액 * 총 예산 및 IT 예산 대비 개인정보 보호 예산 비교	▶ IT 투자액 대비 개인정보 보호 투자 비율
▶ IT 투자액 대비 개인정보 보호 투자 비율의 증가율	▶ 개인정보 보호 투자액의 증가율
▶ 매출액 대비 개인정보 보호 투자 규모	▶ 개인정보 보호를 위한 신규 투자 정도

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

※ 매출액은 별도(또는 개별) 감사보고서 상 금액

※※ 예산 및 실제 집행액은 회사의 내부 보고자료

※※※ IT 투자액은 「정보보호산업의 진흥에 관한 법률」제13조(정보보호 공시)에 따른 정보기술투자액으로 하되, 관련 법령 미적용자는 해당 공시를 준용하여 작성함

※※※※ 정보보호 투자액은 기본적으로 개인정보 보호 투자액으로 인정하나, 정보보호 투자액 중 명확하게 개인정보 보호 투자액에 해당하지 않는 투자액은 제외하며, 상세 산출방법은 별첨자료 참고

※※※※※ 개인정보 보호 예산 및 투자액 고려시, 법 제31조제4항에 따른 CPO의 업무수행과 관련하여 CPO가 해당 예산의 편성·집행 등에의 관여 여부를 주요 고려사항으로 검토할 수 있음

③ 필요 증빙서류

구분	주요 자료
기초자료	▶ 별도(또는 개별)감사보고서, 합계잔액시산표
자산	▶ 자산대장 - 회계연도, 계정과목명, 자산명, 부서명, 당기 감가상각비, 정보기술(IT)투자액 및 개인정보투자액 해당 여부(사유/신규투자 여부 표시)
비용	▶ 비용원장 - 회계연도, 계정과목명, 적요, 부서명, 금액, 정보기술(IT)투자액 및 개인정보투자액 해당 여부(사유/신규 투자 여부 표시)
인건비	▶ 개인정보보호 부문 내부인력의 인건비 내역(급여·상여·퇴직급여·급여성복리후생비), 급여대장, 개인정보보호 부문 인력임을 입증할 수 있는 자료(업무기술서 등), 개인정보보호 전담 확충 증빙(채용 공고, 직무전환 공고 등)
예산서 및 예산 집행 내역	▶ 기안서, 품의서, 지출증빙 등

* 비용이란, 자산의 감가상각비 및 인건비를 제외한 비용을 말하며 개인정보보호투자 목적 용도임을 확인할 수 없는 경우, 해당 용도·목적에 증빙할 수 있는 내부 기안문, 지출결의 등을 추가로 제출하여야 함

④ 참고 사항

■ (정보보호공시 수행 기업) 정보보호 공시 자료를 우선 활용할 수 있으며, 해당 자료를 기준으로 개인정보보호 투자 내역 및 관련 증빙자료를 제출할 수 있다. 이 경우 공시자료 및 관련 증빙자료와 별도(또는 개별)감사보고서 등 최소한의 증빙자료를 통해 확인할 수 있다.

■ (정보보호공시 미수행 기업) 정보보호 공시 가이드라인 상 정보기술 투자액 산정 방법을 참고하여 작성할 수 있다. 이 경우 감사보고서, 합계잔액시산표, 자산대장, 비용원장 등에서 투자내역을 확인할 수 있는 최소한의 증빙자료를 제출하도록 한다.

별첨 개인정보 보호 투자액 산정방법

1 개인정보 보호 부문 판단 기준

■ 개인정보 보호 투자액은 정보보호산업의 진흥에 관한 법률 제 13조(정보보호 공시) 및 관련 규정, 정보보호 공시에 관한 고시를 참고하며, 정보보호 투자금액 중 개인정보 보호 투자에 소요된 비용의 합계를 말한다. 여기에 포함될 수 있는 항목은 다음과 같다.

- ①인건비, ②개인정보 보호시스템 구입비 및 임차료, ③개인정보 보호시스템 유지보수비, ④개인정보 보호 서비스 이용료, ⑤개인정보 보호 외주용역비, ⑥개인정보 보호 컨설팅 비용, ⑦개인정보 보호 교육·훈련비, ⑧개인정보 보호 관련 통신회선 이용료, ⑨기타 개인정보 보호 관련 비용 및 자산 감가상각비 등

※ 정보보호 투자액은 기본적으로 개인정보 보호 투자액으로 인정하나, 명백하게 개인정보 보호와 관련이 없는 부분은 배제하며 정보보호 투자액으로 분류되지 않았으나 개인정보 보호 투자임을 증빙하는 자료를 제출하는 경우 개인정보 보호 관련 투자액으로 추가 인정 가능

2 개인정보 보호 투자항목 산출방법(자산대장/비용원장/인건비)

■ 개인정보 보호 투자액은 ①유·무형자산(감가상각비), ②비용(①·③ 제외), ③ 인건비(내부인력)의 합계로 산출한다. 각 항목은 서로 다른 원천자료(자산대장, 비용원장, 급여자료)에서 추출되며, 동일한 지출이 두 항목에 중복으로 반영되지 않아야 한다.

구성 요소	산출 원천 및 핵심 내용
① 자산	▶ 자산대장에서 개인정보 보호 자산을 구분한 뒤, 해당 자산의 당기 감가상각비(유형 자산), 무형자산상각비, 사용권자산상각비를 합산
② 비용	▶ 비용원장에서 개인정보 보호 관련 비용 계정을 구분한 뒤 해당 금액을 합산 ※ 인건비성 경비·감가상각비 등은 비용원장에서 이중 집계되지 않도록 제외
③ 인건비	▶ 개인정보 보호 내부인력이 확정된 후, 해당 인력의 손익계산서상 급여·상여·퇴직 급여·복리후생비를 인별로 합산 ※ 외주인력 인건비는 별도 산정하지 않고 외주용역비에 포함

최종 집계표 형식은 다음과 같다.

구분	개인정보보호부문 투자액
① 유·무형자산(감가상각비)	
② 비용(①, ③ 제외)	
③ 인건비(내부인력)	
합계	

③ 인건비 추출 방법

- 개인정보 보호 내부인력이 확정된 후, 해당 인력의 손익계산서상 인건비성 경비인 급여, 상여, 퇴직 급여, 복리후생비의 인별 합계를 개인정보 보호 인건비로 산정한다.

인건비 항목	산정 시 유의사항
급여·상여	▶ 연봉계약서 또는 급여대장과 일치하는 손익계산서상 비용만 인정
복리후생비	▶ 4대 보험 회사부담분(근로자 부담분 제외)과 상품권·스톡옵션 등 인별 귀속 가능한 급여성 복리후생비만 포함
퇴직급여	▶ 근속 1년 이상자 대상으로 설정됨

④ 필요 증빙서류

- 정보보호공시를 제출한 기업은 관련 자료를 활용하여 개인정보 보호 투자금액을 소명 가능

항목	필요자료(예시)
투자 현황	▶ 기초자료: 별도(또는 개별)감사보고서, 합계잔액시사표 ▶ 자산: 자산대상(회계연도, 계정과목명, 자산명, 부서명, 당기 감가상각비, 정보 기술(IT)투자액 및 개인정보투자액 해당여부(사유/신규투자여부 표시)) ▶ 비용: 비용원장(회계연도, 계정과목명, 적요, 부서명, 금액, 정보기술(IT)투자액 및 개인정보투자액 해당 여부(사유/신규투자 여부 표시)) ▶ 인건비: 개인정보 보호 부문 내부인력의 인건비 내역(급여·상여· 퇴직급여· 급여성복리후생비), 급여대장, 개인정보 보호 부문 인력임을 입증할 수 있는 자료 (업무기술서 등), 개인정보 보호 전담 확충 증빙(채용 공고, 직무전환 공고 등)
인력 현황	▶ 조직도 ▶ 개인정보 보호부문 인력 명단 (직무, 직렬, 입퇴사일자 포함) 및 개인정보 보호인력 (월평균) ▶ 업무분장표/직무기술서 ※ 정보보호 인력이 개인정보 보호 기능을 동시에 수행하는 것을 인정하되, 만약 정보보호가 아닌 개인정보 보호를 위한 전담 인력에 해당할 시 조직도·업무분장표 등 별도 증빙자료 제출하여 개인정보 보호체계 우수성 요건에서 추가 검토 가능

2 개인정보 보호체계의 우수성

① 주요 내용

- 개인정보 보호를 위한 CEO의 실천의지, CPO의 업무 수행의 충실성·전문성 및 조직·인력의 적정성 등을 감경 요소로 고려

<1. CEO>

- 개인정보의 안전한 처리·정보주체 권리 보호에 대한 CEO의 실천 의지 등을 주요 기준으로 하여 감경 고려요소로 판단
- ※ CEO : 「개인정보 보호법」에서는 개인정보처리자를 공공기관·법인·단체·개인 등으로 규정하고 있으므로 독립된 법인격을 가진 법인의 경우 그 소유주 또는 대표자가 CEO에 해당

[관련규정(「개인정보 보호법」)

제30조의3(사업주 또는 대표자의 책임) 개인정보처리자의 사업주 또는 대표자는 개인정보의 안전한 처리 및 정보주체의 권리 보호에 대한 최종적인 책임자로서 개인정보 보호에 필요한 전문인력과 충분한 예산의 지원 등 총괄적인 관리 조치를 실효성 있게 하여야 한다.

② 세부 고려 사항(예시)

- CEO가 개인정보 보호를 위한 정책 및 전략을 수립하고 관련 사업 목표에 반영하는 등 집행·운영을 총괄하여 관리하고 있는지
- CEO가 개인정보 보호를 기업 경영의 핵심 요소이자 기본 인프라로 인식하고 이를 조직의 정책 결정 및 경영 전반에 반영하고 있는지 판단

[필요 증빙서류]

- 조직 내 개인정보 처리·보호를 위한 정책 또는 전략(구성 내용, 타 사업부문 전략과의 우선순위, 최종 결재자 등), KPI, 개인정보보호 활동 내역(행사 참여, CEO 서한 등) 등

- 개인정보 보호를 위한 실효적인 관리체계의 구축 여부
- 개인정보 보호를 위한 전담 조직체계 구축, 전문인력 배치와 관련 예산 편성 과정에 CEO가 적극적으로 참여하고 적정성 점검 등을 수행하는지 판단
- CPO가 개인정보 처리 및 보호에 대한 주요 사항에 대해 이사회 및 대표자에게 직접 보고할 수 있는 체계 운영의 충실성

[필요 증빙서류]

- 개인정보 보호 분야 유관 자격 및 경력을 갖춘 전문인력 현황 및 개인정보 보호를 위한 시스템 · 예산 등 규모, 개인정보 보호 인력 및 예산 계획에 대한 CEO 보고 내역, CPO 보고 및 조직 체계, 이사회 안건 내역 등

[관련규정]

「개인정보 보호법」

제31조(개인정보 보호책임자의 지정 등) ⑦ 개인정보처리자는 개인정보 보호책임자가 제3항 각 호의 업무를 수행함에 있어서 정당한 이유 없이 불이익을 주거나 받게 하여서는 아니 되며, **개인정보 보호책임자가 업무를 독립적으로 수행할 수 있도록 보장하여야 한다.**

「개인정보 보호법 시행령」

제32조(개인정보 보호책임자의 업무 및 지정요건 등) ① ~ ⑤ (생 략)

⑥ **개인정보처리자(법 제31조제2항에 따라 사업주 또는 대표자가 개인정보 보호책임자가 되는 경우는 제외한다)**는 법 제31조제6항에 따른 **개인정보 보호책임자의 독립성 보장**을 위해 다음 각 호의 사항을 준수해야 한다.

1. 개인정보 처리와 관련된 정보에 대한 개인정보 보호책임자의 접근 보장
2. 개인정보 보호책임자가 개인정보 보호 계획의 수립 · 시행 및 그 결과에 관하여 정기적으로 대표자 또는 이사회에 직접 보고할 수 있는 체계의 구축
3. 개인정보 보호책임자의 업무 수행에 적합한 조직체계의 마련 및 인적 · 물적 자원의 제공

■ CEO가 조직의 **경영 목표 및 사업 추진 시 개인정보 보호 원칙을 반영**하고 **대내외 홍보** 등을 통해 개인정보 보호 **실천 의지를 표명**하고 있는지

- CEO가 조직의 **개인정보 문화 확산 촉진**을 위한 **활동**(캠페인, 포상 등)에 직접 참여하고 경영 · 사업 목표 등에 **개인정보 관련 지표 설정 여부** 판단

[필요 증빙서류]

- 기업 내 개인정보 보호 활동(캠페인, 행사, 선포식, 표창 등) 내역, KPI 등

〈2. CPO〉

■ CPO가 조직 내 개인정보 처리에 관한 업무를 총괄해서 담당할 수 있도록 **CPO의 업무수행의 충실성, 전문성 등을** 감경 요소로 판단

③ 세부 고려 사항(예시)

■ CPO의 업무 수행의 충실성

업무	주요 내용(예시)
1. 개인정보 거버넌스 구축 및 운영	▶ 개인정보 보호 관련 부서의 협업 체계 구축 여부 ▶ 전사적인 개인정보 위험 파악·관리 절차 구축 여부
2. 개인정보 처리환경 분석 및 관리	▶ 조직 내 서비스·시스템 별로 처리하는 개인정보의 생명주기를 파악한 후 개인정보 흐름도를 최신화 ▶ 조직 내 처리되는 개인정보 파일의 현황에 대해 주기적 확인
3. 개인정보 보호 활동	▶ 개인정보 수집·이용 또는 제3자 제공에 대한 적법성 검토 및 관리·감독 ▶ 처리 중인 개인정보가 목적을 달성하거나 보유기간이 경과되면 파기할 수 있는 절차 마련 및 이행에 대한 관리·감독 ▶ 정보주체의 권리보장을 위한 표준화된 대응 절차 수립 및 처리 현황의 주기적 점검 ▶ 전사적 개인정보 보호활동 이행현황을 주기적으로 파악하고 주요 사항에 대해서는 경영진 대상으로 보고 후 개선조치 마련 ▶ 개인정보파일을 체계적으로 관리하기 위한 전차 마련 및 일제 정비를 통해 최신성 유지할 수 있도록 관리·감독 ▶ 개인정보 국외 이전에 관한 적법성 검토 및 국회 이전시 보호 조치 마련 여부 등
4. 개인정보 활용 안전조치 및 관리감독	▶ 개인정보 위험을 체계적으로 식별·평가할 수 있도록 조직의 환경에 맞는 위험 평가 절차 마련 여부 ▶ 조직의 특성에 맞는 가명정보 관리계획의 수립
5. 개인정보 침해 대응 및 대외 협력	▶ 개인정보 유출 사고 대응 체계(보고체계, 사고 대응팀, 매뉴얼 등) 구축 ▶ 고객센터 및 개인정보 보호 조직간 개인정보 침해 민원 전달을 위한 신속 전달체계 구축 ▶ 인사 규정에 개인정보 보호 정책 위반에 대한 징계 절차 반영

[필요 증빙서류]

- CPO 직무기술서, 업무별 처리 증빙자료, 보고 내역 등

[관련규정(「개인정보 보호법」)

제31조(개인정보 보호책임자의 지정 등) ④개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

1. 개인정보 보호 계획의 수립 및 시행
 2. 개인정보 보호에 필요한 전문 인력의 관리 및 예산의 확보
 3. 사업주 또는 대표자 및 이사회에 대한 개인정보 보호 현황 및 주요 사항의 보고
 4. 개인정보 처리 및 보호의 실태와 관행에 대한 정기적인 조사 및 개선
 5. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
 6. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
 7. 개인정보 보호 교육 계획의 수립 및 시행
 8. 개인정보파일의 보호 및 관리·감독
 9. 그 밖에 개인정보의 적절한 처리 및 보호를 위하여 대통령령으로 정한 업무
- ⑤ 개인정보 보호책임자는 제4항 각 호의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 **수시로 조사하거나 관계 당사자로부터 보고**를 받을 수 있다.
- ⑥ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 **즉시 개선조치**를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 **개선조치**를 보고하여야 한다

■ CPO의 자격 및 권한 등의 우수성

- CPO의 **직급** 및 법적 자격요건* 이외 **추가적 자격요건**을 가지고 있는지

* 개인정보 보호·정보보호·정보기술 경력을 합하여 4년 이상 보유(개인정보보호 경력 최소 2년 이상)

- 자격요건을 갖춘 **전문CPO 지정기관이 아님에도** 개인정보 보호·정보보호·정보기술 경력을 갖춘 **CPO를 지정하고 있는지** 판단

- CPO가 기업 내 **최상위 의사결정기구**에 참여하는지 여부

[필요 증빙서류]

- CPO 직무기술서, 경력 및 자격사항, CPO의 개인정보 관련 수상 및 표창, 최상위 의사결정기구 운영 규정·회의소집 공문 등

[관련규정(「개인정보 보호법 시행령」)

제32조(개인정보 보호책임자의 업무 및 지정요건 등) ④ 다음 각 호의 어느 하나에 해당하는 개인정보처리자(공공기관의 경우에는 제2조제2호부터 제5호까지에 해당하는 경우로 한정한다)는 제3항 각 호의 구분에 따른 사람 중 별표 1에서 정하는 요건을 갖춘 사람을 개인정보 보호책임자로 지정해야 한다.

1. 연간 매출액등이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자(제2조제5호에 따른 각급 학교 및 「의료법」 제3조에 따른 의료기관은 제외한다)
 - 가. 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자
 - 나. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자
2. 직전 연도 12월 31일 기준으로 재학생 수(대학원 재학생 수를 포함한다)가 2만명 이상인 「고등교육법」 제2조에 따른 학교
3. 「의료법」 제3조의4에 따른 상급종합병원
4. 공공시스템운영기관

〈3. 조직·인력의 적정성〉

- 개인정보처리자(기업·기관)가 개인정보의 안전한 처리·보호를 위해 갖추고 있는 **조직·인력 체계의 성숙도 여부**를 감경 요소로 판단

④ 세부 고려 사항(예시)

- 개인정보보호 업무 **종사자의 전문성 및 처우 수준**

- 개인정보 보호 관련 **자격 및 경력**을 갖춘 자를 전담·담당인력으로 배정
- 개인정보 전담·담당인력에 대한 **전문성 강화 및 처우**(평가 가점, 수당 등) **개선에 대한 노력**

[필요 증빙서류]

- 개인정보 보호 인력 현황(경력 및 자격 등), 인사관리 체계, 자격증 및 학위 취득 지원 현황, 개인정보 보호 인력 직무 기술서 등

[관련규정(「개인정보 보호법 시행령」)

제32조(개인정보 보호책임자의 업무 및 지정요건 등) ① ~ ⑤ (생 략)

⑥ 개인정보처리자(법 제31조제2항에 따라 사업주 또는 대표자가 개인정보 보호책임자가 되는 경우는 제외한다)는 법 제31조제6항에 따른 개인정보 보호책임자의 독립성 보장을 위해 다음 각 호의 사항을 준수해야 한다.

1. 개인정보 처리와 관련된 정보에 대한 개인정보 보호책임자의 접근 보장
2. 개인정보 보호책임자가 개인정보 보호 계획의 수립·시행 및 그 결과에 관하여 정기적으로 대표자 또는 이사회에 직접 보고할 수 있는 체계의 구축
3. 개인정보 보호책임자의 업무 수행에 적합한 **조직체계의 마련 및 인적·물적 자원의 제공**

- 개인정보 보호 업무가 효율적으로 수행될 수 있도록 **충분한 인력이 지원되고 있는지 여부**

- 개인정보 관련 위험이나 이슈에 대해 **전사적으로 전파하고 선제적으로 관리하는 체계 마련 여부**

[필요 증빙서류]

- 조직도, 조직 내 개인정보 보호 조직·시스템 유무, 직제 및 편제, 역할·기능 등

3 안전조치 확보를 위한 추가적 노력

① 주요 내용

■ 개인정보의 안전성 확보조치 기준(이하 ‘안전조치 고시’)에서 정하고 있는 안전조치를 **기준 이상으로 적용한 경우**를 과징금 감경 요소로 고려

- 개인정보 유출등이 발생한 시점에 해당 개인정보처리시스템에 적용·운영되고 있는 안전조치를 중심으로 고려
- 단, 추가적 안전조치가 개인정보처리자의 실질적 조치로 적용되어 있음을 입증 가능하도록 **내부 관리 계획에 명문화**하고, 관련 사항 등이 증빙을 통해 확인되어야 함

※ 내부 관리계획의 하위 지침을 증빙자료로 제출할 경우, ①내부관리계획에 위임규정이 있으며, ②CPO이상 결재를 받고, ③사고 전 공식적인 문서로 시행되고 있음을 입증하여야 함

■ 개인정보의 안전성 확보를 위하여 ① **추가적 안전조치***를 적용한 경우, ②추가로 적용한 안전조치 요소가 개인정보 유출등에 따른 2차 피해 최소화 또는 확산 방지 등에 기여한 경우**를 과징금 감경 요소로 고려

* 안전조치 고시에서 규정한 기준 이상의 강화된 안전조치를 적용하거나, 명시적으로 규정되지 않은 안전조치를 추가적으로 적용한 경우 등

** 추가적 안전조치를 위한 노력이 개인정보 유출을 조기에 탐지하고 확산 차단으로 이어진 경우 등

② 세부 고려 사항(예시)

가. 추가적 안전조치를 적용한 경우

1) 내부 관리계획 이행실태의 지속적 점검·개선

■ 개인정보 보호책임자 주도로 내부 관리계획의 이행 실태를 짧은 주기로 충실히 점검하고 지속적인 개선 활동을 수행한 경우

[관련 규정]

안전조치 고시 제4조(내부 관리계획의 수립·시행 및 점검) ④ 개인정보 보호책임자는 접근 권한 관리, 접속 기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상 점검·관리하여야 한다.

[예시]

- 내부 관리계획의 이행 실태 점검을 매월 수행하고 발견된 문제점에 대한 근본원인 분석 및 개선조치를 적시에 수행함. 또한, 그 결과를 개인정보 보호책임자 및 CEO에게 보고하고 지속적으로 관리함
- 개인정보 처리 과정에서 발생할 수 있는 위험을 식별·분석·평가하고, 그 결과에 따른 위험을 감소시키기 위한 체계를 내부 관리계획에 반영함. 또한, 위험관리 및 조치 현황을 개인정보 보호책임자 및 CEO에게 보고하고 지속적으로 점검·관리함

[필요 증빙서류]

- 내부 관리계획 이행 실태 점검 계획
- 내부 관리계획 이행 실태 점검 결과 보고서(개인정보 보호책임자 및 CEO 보고 증적 포함)
- 위험평가 등에 따른 개선조치 및 이행점검 결과

2) 접근 권한의 체계적 및 자동화된 관리

- 임직원 뿐만 아니라 임시직원, 협력사 직원 등 외부자를 포함한 모든 개인정보취급자를 대상으로 체계적이고 자동화된 접근 권한 관리체계를 수립·이행한 경우

[관련 규정]

안전조치 고시 제5조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 한다.
 ② 개인정보처리자는 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

[예시]

- 통합 계정 및 접근 권한 관리시스템을 구축하여 응용프로그램, 서버, DBMS를 포함한 모든 개인정보처리시스템의 계정 및 접근 권한을 통합 관리함
- 인사시스템과 연동하여 인사 변동 내역이 개인정보처리시스템의 계정 및 접근 권한에 신속히 반영될 수 있도록 자동화함
- 임시직원, 협력사 직원 등 외부자용 계정관리시스템을 구축하고 이를 개인정보처리시스템과 연동하여 외부자의 인사 및 업무 변동 내역이 개인정보처리시스템에 즉시 반영될 수 있도록 함
- 접근 권한의 적절성 여부를 제로트러스트 관점에서 지속적으로 점검

[필요 증빙서류]

- 계정 및 접근 권한 관리 지침 및 절차서
- 계정 및 접근 권한 관리시스템 현황
- 계정 및 접근 권한 검토 보고서

3) 안전한 인증수단 확대 적용

- 계정 도용 및 탈취 위험을 원천적으로 줄이기 위해 외부망 뿐만 아니라 내부망에서 개인정보처리시스템 접속시에도 안전한 인증수단을 적용한 경우

[관련 규정]

안전조치 고시 제6조(접근 통제) ② 개인정보처리자는 개인정보처리시스템에 대한 정당한 접근 권한을 가진 자(다만, 정보주체는 제외한다)가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다. 다만, 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있다.

[예시]

- 외부에서 개인정보처리시스템 접속시 안전한 인증수단과 안전한 접속수단 동시 적용
- 내부에서 개인정보처리시스템 접속시에도 안전한 인증수단 적용

[필요 증빙서류]

- 네트워크 구성도
- 안전한 인증수단 적용 현황

4) 공격표면에 대한 체계적 관리 및 상시적 취약점 점검·조치

■ 외부에 공개된 자산, Shadow IP 등 공격표면에 대한 체계적이고 자동화된 관리대책을 수립
· 이행하고, 최신 취약점에 의한 공격을 선제적으로 예방할 수 있도록 취약점 점검을 고도화
된 방식으로 상시 수행하고 이에 따른 개선조치를 신속히 수행한 경우

[관련 규정]

안전조치 고시 제6조(접근 통제) ③ 개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유
설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의
컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.

[예시]

- 자체 취약점 점검조직(외부 전문기업 포함)을 구성하고, 모의침투 테스트를 포함하여 상시적 또는 짧은
주기로 취약점 점검을 수행하고 발견된 취약점에 대해 지체없이 조치
- 자동화된 방법으로 공격표면을 탐지·관리(공격표면 최소화 등 후속조치 수행)
- AI를 통한 취약점 점검 등 취약점 점검방법 고도화
- 취약점 신고조치 공개제도(CVD·VDP)에 상시 참여
- 버그 바운티 제도 운영

[필요 증빙서류]

- 네트워크 구성도
- 정보자산 관리현황(공격표면 관리현황 포함)
- 정보자산 현행화 관리 절차
- 취약점 점검 계획
- 취약점 점검 결과(개선조치에 관한 사항 포함)
- 보안 취약점 신고·조치·공개제도(CVD·VDP)에 참여 증적

5) 암호화 대상 개인정보 항목 확대 적용

■ 개인정보 유·노출 및 이에 따른 2차 피해를 최소화하기 위해 **법적 암호화 의무 대상 항목 외에도 다수의 개인정보 항목을 안전한 암호 알고리즘으로 암호화** 하여 저장한 경우

[관련 규정]

안전조치 고시 제7조(개인정보의 암호화) ① 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 **안전한 암호 알고리즘으로 암호화**하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

② 개인정보처리자는 **다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장**하여야 한다.

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 생체인식정보

③ 개인정보처리자는 이용자가 아닌 정보주체의 개인정보를 다음 각 호와 같이 저장하는 경우에는 암호화하여야 한다.

1. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우
2. 내부망에 고유식별정보를 저장하는 경우(다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다)
 - 가. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
 - 나. 암호화 미적용시 위험도 분석에 따른 결과

[예시]

- 안전조치 고시 제7조 제1항, 제2항 및 제3항 등에서 정하는 암호화 대상 개인정보 외에 이름, 휴대폰번호, 이메일주소, 생년월일, 집주소 등 개인정보 보호 강화를 위하여 추가적인 암호화가 필요하다고 판단한 개인정보를 안전한 암호 알고리즘*으로 암호화

* (예시) 일방향 암호 알고리즘, 대칭키 암호 알고리즘, 공개키 암호 알고리즘

[필요 증빙서류]

- 암호화 관련 내부 지침
- 암호화 적용 현황

6) 원천적인 암호키 유출방지 기술 적용

- 암호키에 대한 불법적 접근 및 유출을 구조적으로 방지할 수 있도록 기술적 보안대책을 적용한 경우 등

[관련 규정]

안전조치 고시 제7조(개인정보의 암호화) ⑥ 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업 · 중견기업 · 공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업 · 단체에 해당하는 개인정보처리자는 **암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립 · 시행**하여야 한다.

[예시]

- 하드웨어 보안모듈(HSM, Hardware Security Module)을 통해 암호키를 생성 · 보관 · 이용 · 폐기하도록 하여 암호키에 대한 불법적 접근 및 유출을 근본적으로 방지한 경우

[필요 증빙서류]

- 암호키 관리 내부지침
- HSM 도입 내역 등

7) 개인정보 접속기록 등 관련 로그에 대한 보관 · 점검 등 관리 강화

- 개인정보의 오 · 남용, 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손 등에 효과적으로 대응하고 사고 발생시 신속한 원인분석이 가능하도록 **관련 로그를 장기간 안전하게 보관하고, 고도화된 방식으로 모니터링 · 분석 및 점검을 수행**한 경우

[관련 규정]

안전조치 고시 제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보처리시스템에 접속한 자(다만, 정보주체는 제외한다)의 접속기록을 1년 이상 보관 · 관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관 · 관리하여야 한다.

- ② 개인정보처리자는 개인정보의 오 · 남용, 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손 등에 대응하기 위하여 개인정보취급자의 개인정보처리시스템에 대한 접속기록 및 개인정보 다운로드 상황을 확인하고 점검하는 주기 · 방법 · 사후조치절차 등을 내부 관리계획으로 정하고 이행하여야 한다.
- ③ 개인정보처리자는 접속기록이 위 · 변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다.

[예시]

- 네트워크 장비의 로그기록, 보안시스템의 로그기록 등을 접속기록에 준한 기간 동안 보관
- 접속기록을 법적 요건 이상으로 장기간 보관
- 통합 로그관리시스템을 통해 개인정보처리시스템 및 정보통신망을 관리하는 시스템 등의 로그기록을 실시간으로 통합하여 저장·관리 및 고도화된 방법으로 분석
- 인공지능 등 기술을 활용한 (준)실시간 이상행위 탐지 및 대응

[필요 증빙서류]

- 접속기록 관련 내부 지침
- 접속기록 및 로그기록 보관 내역
- 접속기록 점검 내역
- 로그관리시스템 현황

8) S/W 공급망 및 보안패치에 대한 체계적 관리

- 오픈소스를 포함하여 S/W 공급망 현황을 지속적으로 식별·관리하고 보안 업데이트 공지가 있는 경우 이를 최대한 신속하게 적용할 수 있도록 절차를 수립·이행한 경우

[관련 규정]

안전조치 고시 제9조(악성프로그램 등 방지) ② 개인정보처리자는 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 이에 따른 업데이트 등을 실시하여야 한다.

[예시]

- 공급망 보안 관리체계를 수립하고 공급망으로부터 발생 가능한 위험을 지속적으로 모니터링 및 검토
- 개인정보처리시스템 등에 활용하기 위하여 구매하거나 개발한 소프트웨어의 SBOM(Software Bill of Materials)을 확보 또는 작성하고, 이를 현행화하여 관리
- 개인정보처리시스템 전체 구성요소에 대해 EOS(End of Service) 및 패치 적용 현황을 식별하여 관리하고, EOS 시점이 도래하기 전에 장비 또는 소프트웨어 교체 등 선제적 대응

[필요 증빙서류]

- 공급망 보안 관련 지침
- 패치관리 지침
- SBOM
- EOS 및 패치 적용 현황

나. 개인정보 유출·피해 확산방지에 기여

■ 적용한 추가적 안전조치가 개인정보 유출·피해 확산방지에 기여한 사실을 입증한 경우
감경요소로 검토

[예시]

- 법적 암호화 의무대상 외의 개인정보가 암호화된 상태로 유출되어 2차 피해가 최소화된 경우
- 취약점 점검·모의침투테스트 등(CVD·VDP 포함)을 통해 발견된 취약점을 수정하였으며, 해당 취약점이
기 신고된 사고의 개인정보 유출·피해 확산방지에 기여한 경우
- 네트워크 장비, 보안시스템의 상세한 로그기록 및 고도화된 모니터링 체계를 통해 개인정보 유출 징후
를 파악하고 이를 신속히 차단하여 피해확산 방지에 기여한 경우

과징금 투자 감경제도 안내서

발 행 일 2026년 9월
발 행 처 개인정보보호위원회

※ 최신자료는 “개인정보보호위원회 누리집(pipc.go.kr)”, “개인정보 포털(privacy.go.kr)”에서 확인할 수 있습니다.

과징금 투자 감경제도 안내서



개인정보보호위원회

personal Information Protection Commission