NEWS LETTER

2025-09-30

Legal Issue

- SKT 과징금 1,347억원 어떻게 산정됐나
- 개인정보의 안전성 확보조치 기준 개정안 분석: 데이터 시대, 기업의 개인정보 보호 책임 강화와 전략적 대응 방안

MINWHO News

- 최주선 변호사, K-CPO 컨퍼런스 참가해 '개인정보 관련 처분 사례 분석' 발표
- 김경환 변호사, '포장도 법적 보호 대상' 메로나 표절 분쟁 법리해석 관련 인터뷰
- 양진영 변호사, AI윤리협의체 포럼 'AI 정서 교감의 법적 쟁점' 발표자로 참여

Business CASE

법무법인 민후

법무법인 민후

Legal Issue

SKT 과징금 1,347억원 어떻게 산정됐나

김경환 대표변호사

SK텔레콤(SKT)에게 역대 최대의 과징금인 1347억9100만원이 부과됐다. 관련해서 과징금이 어떻게 산정되는지의 질문을 많이 받고 있는데, 여기서는 SKT 과징금 1347억원이 어떻게 산정됐는지를 살펴보고자 한다.

과징금의 근거 조문은 개인정보보호법 제64조의2이지만, 구체적인 산정은 '개인정보 보호법 위반에 대한 과징금 부과기준'에 의한다. 개인정보보호위원회(보호위원회)는 개인정보보호법 제64조의2 제1항의 9개 사유에 해당하는지 정밀한 검토를 거친 다음, 과징금 부과 여부를 결정한다. 다만 위반행위의 내용·정도가 경미하거나 사소한 부주의나 오류로 인한 위반행위인 경우, 정보주체에게 피해가 발생하지 아니했거나 경미한 경우 등은 법 위반행위가 있어도 과징금이 부과되지 않는다.

과징금 부과가 결정된 경우, 첫 단계로 '전체 매출액'을 계산한다. 전체 매출액이란 위반행위가 있었던 사업연도의 직전 3개 사업연도의 연평균 매출액이고, 총 매출액에서 부가가치세, 매출할인, 매출환입, 매출에누리 등을 차감한 순매출액으로 산정한다. SKT의 경우 약 17조의 매출액이 전제됐다.

이후 전체 매출액에서 위반행위와 관련이 없는 매출액을 공제해 '관련 매출액'을 산정하는데, 예컨대 개인정보 처리와 관련이 없는 B2B 매출 등이 대표적이다. SKT의 경우, 과징금 산정의 기준이 되는 매출액은 SKT 전체 매출액에서 위반행위와 관련 없는 부분을 제외한 '전체 이동통신서비스 매출액'이었다.

관련 매출액이 나오면 '기준금액'을 정한다. 기준금액은 위반행위와 관련된 매출액에 위반행위의 중대성에 따른 부과기준율을 곱해 산출하는데, 중대성 판단에 대해서는 매우 중대함, 중대함, 보통, 약함의 4단계의 값이 존재하고, 그에 따라서 부과기준율이 0.03%에서 2.7%까지 곱해진다.

보호위원회는 이번 유출 사고가 △다수의 안전조치 의무 위반이 직접적 원인이 된 점 △가입자 인증에 필요한 핵심 정보(유심 인증키 등)가 유출된 점 △약 2300만명의 대규모 개인정보가 유출된 점 등을 고려하여 '매우 중대한 위반행위'로 판단했다. 이 판단에 따라 높은 부과기준율이 적용돼 높은 기준금액이 설정됐다.

다음으로 '1차 조정' 단계에서는 위반 기간, 위반 횟수 등을 고려해 기준금액을 가중하거나 감경한다. SKT의 경우, 위반행위가 2년을 초과해 장기간 지속된 점이 가중 사유로 고려됐다.

'2차 조정' 단계에서는 조사 협조 여부, 피해 구제 노력 등을 종합적으로 고려해 1차 조정 금액을 다시 가감한다. SKT는 △유출 사고와 관련된 위반행위를 시정한 점 △이용자의 피해 회복을 위해 노력한 점 △기타 개인정보 보호를 위한 노력을 기울인 점 등이 참작돼 과징금이 일부 감경됐다.

마지막으로 '부과과징금의 결정' 단계에서는 위반행위자의 현실적 부담 능력 등을 고려해 최종 금액을 결정하게 된다.

이러한 다단계 산정 과정을 통해, '매우 중대한 위반'으로 설정된 높은 기준금액에서 위반 기간에 따른 가중과 시정 노력 등에 따른 감경 요소를 종합적으로 반영해 최종 과징금 1347억9100만원이 결정됐다. 매출액 자체가 워낙 큰 점을 고려하면, SKT 입장에서는 나름 선방한 것으로 평가된다.

바람직하게는 개인정보 유출사고를 피할 수 있으면 좋지만, 일단 개인정보 유출 사고가 나더라도, 사후적인 보호 조치나 피해 회복 노력 등도 과징금 산정시 감안되는 점도 이 기회에 유념하면 도움이 될 것으로 보인다.

김경환 대표변호사, 변리사

프로필 보기

02-532-3425
oalmephaga@minwho.kr

Legal Issue

개인정보의 안전성 확보조치 기준 개정안 분석:
데이터 시대, 기업의 개인정보 보호 책임 강화와 전략적 대응 방안

현수진 변호사

지난 7월 21일 개인정보 보호위원회는 인공지능(AI)과 클라우드 컴퓨팅 기술의 급격한 발전, 그리고 데이터 중심 사회로의 전환이라는 시대적 요구에 발맞춰 「개인정보의 안전성 확보조치 기준」(이하 '고시') 일부 개정안을 행정예고하였다.

이번 개정은 단순히 기존 규정의 보완을 넘어, 변화하는 디지털 환경 속에서 개인정보 보호의 실효성을 높이고 개인정보처리자의 책임성을 한층 더 강화하려는 정부의 강력한 의지를 반영하고 있다. 최근 발생한 SKT 사건과 같이 개인정보 유출사고가 발생한 경우, 기업의 귀책사유가 어느정도인지를 판단할 때에는 안전성 확보조치 기준이 매우 중요하게 작용한다. 이러한 관점에서, 사업자의 입장에서는 이번 개정안이 가져올 변화의 폭과 깊이를 정확히 이해하고, 선제적으로 대응하는 것이 그 어느 때보다 중요해졌다.

1. 개정 배경: 변화하는 디지털 환경과 규제의 패러다임 전환

고시 개정의 가장 큰 배경은 바로 인공지능, 클라우드 등 신기술의 확산으로 인한 개인정보 처리 환경의 복잡성 증가이다. 기존 고시는 주로 온프레미스(On-premise) 환경에서의 개인정보 보호를 상정하고 있었으나, 이제는 다양한 클라우드 서비스와 AI 모델 학습 등 유연하고 분산된 환경에서 개인정보가 처리되는 것이 일반화되었다. 또한, 오픈마켓 판매자, 플랫폼 입점업체 등 기존 '개인정보취급자'의 정의에 명확히 포섭되지 않아 규제의 사각지대에 놓였던 개인정보 처리 주체들에게도 안전성 확보 의무를 명확히 부과함으로써, 개인정보 보호의 빈틈을 메우고자 하는 목적이 크다.

이번 개정은 단순히 규제 강화의 측면에서 바라볼 수도 없다. 개인정보처리자가 각자의 개인정보처리 환경을 고려하여 '위험 분석'을 실시하고, 그 결과에 따라 안전성 확보 조치를 차등화할 수 있도록 함으로써, 기업의 자율성과 효율성을 동시에 고려하려는 패러다임 변화 또한 담고 있다.

이는 획일적인 규제 적용을 넘어, 기업 스스로의 위험 관리 역량을 높이도록 유도하는 규제 패러다임 전환의 시그널로 해석된다.

2. 주요 개정 내용 및 기업의 주목 포인트

1) 용어 정의의 명확화 및 적용 대상 확대

▶ '비밀번호'의 개념 변경 (제2조 제8호)

기존 고시에서는 "비밀번호"란 정당한 접속 권한을 가진 자라는 것을 "식별"할 수 있는 고유의 문자열로 정의되었다. 이번 개정안에서는, 비밀번호의 목적을 접속 권한을 "인증"하기 위한 것으로 변경되었다.

이는 단순히 계정 확인을 넘어, 접속 권한을 가진 자가 '누구인지'를 검증하는 행위의 중요성을 강조하는 것으로, 더 강력한 인증 수단의 도입을 유도한다.

▶ '개인정보처리시스템에 접속하는 자'로의 적용대상 확대

기존 고시에서 '개인정보취급자'에게만 적용되던 접근 권한 관리(제5조), 접근 통제(제6조), 접속기록 보관(제8조) 등의 의무가 '개인정보처리시스템에 접속한 자(정보주체는 제외)' 또는 '정당한 권한을 가진 자' 등으로 확대됩니다.

이는 오픈마켓 판매자나 클라우드 서비스를 통해 개인정보를 처리하는 협력업체 직원 등, 직접적인 고용 관계는 없으나 개인정보처리시스템에 접근하여 개인정보를 처리하는 모든 관계자에게까지 안전성 확보 의무가 적용됨을 의미한다. 기업은 자사의 개인정보 처리 흐름을 전면적으로 재검토하여, 개인정보취급자 외의 다양한 '접속자' 그룹을 식별하고 이들에게도 고시에 상응하는 안전성 확보 조치를 적용하고 관리할 체계를 구축해야 한다.

2) 내부 관리계획의 재정비 필요성 강조 (제4조)

개정안은 '출력·복사 시 안전조치(제12조)' 및 '개인정보의 파기(제13조)'에 관한 사항을 내부 관리계획의 필수 포함 사항으로 추가하여 명시한다. 개인정보의 생명주기(수집-이용-제공-파기) 전반에 걸친 관리가 얼마나 중요한지를 보여준다.

특히 개인정보 파기는 그간 소홀히 다뤄지기 쉬웠던 영역인데, 이제는 내부 관리계획에 명확한 절차와 기준을 포함하고 주기적으로 점검해야 하며, 문서 형태로 출력되거나 복사되는 개인정보에 대한 통제도 강화해야 한다.

다. 인터넷망 차단 조치의 유연화 및 책임성 강화 (제6조의2 신설)

일일 평균 100만 명 이상 이용자 개인정보를 처리하는 개인정보처리자는 개인정보처리시스템 접근 권한 설정, 개인정보 다운로드 또는 파기 권한을 가진 자의 컴퓨터 등에 대해 인터넷망 차단 조치를 해야 한다. 그러나, 예외 조항을 두어 내부 관리계획에 따른 위험 분석 결과 위험이 현저히 낮거나, 위험을 감소시킬 수 있는 보호 조치(예: 이중인증, 망 분리 대체 정보보호통제 등)를 적용한 경우에는 인터넷망 차단 조치를 하지 않을 수 있다. 단, 민감정보 또는 고유식별정보를 다운로드하거나 파기할 수 있는 취급자의 컴퓨터 등에는 예외를 적용하지 않는다.

이 조항은 클라우드 환경 도입 등으로 인해 획일적인 망 차단이 현실적으로 어려운 기업들에게 숨통을 열어줄 수 있다. 그러나 '위험 분석'이라는 전제 조건이 붙어 있으며, 특히 민감정보 등 중요 정보에 대해서는 예외가 없다는 점을 명심해야 한다. 기업은 자사의 IT 환경과 개인정보 처리 특성을 면밀히 분석하고, 내부 관리계획에 따라 체계적인 위험 분석 절차와 기준을 마련해야 하고, 단순히 인터넷망 차단 의무를 면제받기 위한 형식적인 위험 분석이 아닌, 실질적인 위험 평가와 그에 상응하는 '대체 정보보호통제' (예: 다단계 인증, 접근 제어 강화, 비정상 행위 탐지 시스템 도입 등)를 구축하고 문서화하는 것이 핵심이다.

4) 접속기록 관리 의무의 실질적 확대 (제8조)

접속기록 보관 대상이 '개인정보취급자'에서 '개인정보처리시스템에 접속한 자(정보주체 제외)'로 확대된다. 또한, 접속기록의 점검 주기, 방법, 사후 조치 절차 등을 내부 관리계획으로 자율적으로 정하고 이행하도록 하여 책임추적성을 확보한다.

앞서 적용대상의 확대 항목에서 언급한 바와 같이, 이제는 개인정보처리시스템에 접근하는 모든 내부 인력(정규직, 계약직, 파견직 등)뿐만 아니라, 외부 개발자, 유지보수 인력, 클라우드 관리자 등 권한을 가진 모든 '접속자'의 행위가 기록되고 관리되어야 한다.

또한, 단순히 기록만 하는 것을 넘어, 기록의 위변조 방지, 안전한 보관, 그리고 월 1회 이상의 정기적인 점검 및 개인정보 다운로드 등 비정상 행위 발생 시 사유 확인 등 실질적인 분석과 사후 조치가 매우 중요해졌다. 침해 사고 발생 시 책임 소재 규명 및 원인 분석의 핵심 증거가 되므로, 접속기록 관리 시스템의 고도화 및 운영 인력의 전문성 강화가 요구된다.

3. 기업의 전략적 대응 방안 및 결론

이번 「개인정보의 안전성 확보조치 기준」 개정안은 기업에게 개인정보 보호에 대한 더욱 엄중한 책임을 요구하면서도, 변화된 기술 환경을 고려한 유연성을 일부 제공하고 있다. 기업은 이를 단순한 규제 강화로 인식하기보다, 개인정보 보호 시스템을 고도화하고 기업 경쟁력을 강화하는 기회로 삼아야 한다.

▶ 전사적 개인정보 관리 체계 재점검

개인정보 생명주기 전반에 걸쳐 개인정보가 어디에 있고, 누가 접근하며, 어떻게 처리되고, 언제 파기되는지 명확히 파악하는 '개인정보 흐름도'를 업데이트하고, 이에 기반하여 내부 관리계획 및 관련 지침을 개정안에 맞춰 전면 재정비해야 한다. 특히 기존 '개인정보취급자' 외의 '접속자' 그룹을 식별하고 이들에 대한 관리 방안을 수립해야 한다.

▶ 접근 통제 및 인증 시스템 강화

단순히 비밀번호 정책 준수를 넘어, 다단계 인증(MFA), 생체 인증 등 더욱 강력하고 안전한 인증 수단을 도입하는 것을 적극 검토해야 한다. 또한, 접근 권한 부여 시 '최소 권한의 원칙(Principle of Least Privilege)'을 엄격히 적용하고, 불필요한 접근 권한은 즉시 회수하는 체계를 갖춰야 한다.

▶ 위험 기반의 보안 투자 및 유연한 망 관리:

인터넷망 차단 조치 의무의 유연화는 기업에게 부담 완화와 동시에 '위험 분석'이라는 새로운 책임을 부여한다. 기업은 전문적인 위험 분석을 수행하여 자사의 개인정보처리 환경에 맞는 최적의 보안 조치를 수립해야 한다. 무작정 망 차단 의무 면제를 추진하기보다, 충분한 위험 분석과 그에 상응하는 강력한 대체 통제 수단을 마련하는 데 투자를 아끼지 않아야 한다. 특히 클라우드 환경에서는 클라우드 보안 형상 관리(CSPM), 클라우드 워크로드 보호 플랫폼(CWPP) 등 클라우드 환경에 특화된 보안 솔루션 도입을 고려하는 것이 좋다.

▶ 로그 관리 및 모니터링 체계 고도화

접속기록은 개인정보 유출 사고 발생 시 가장 중요한 증거가 된다. 단순히 법적 의무 준수를 넘어, 통합 로그 관리 시스템(ELK Stack 등) 구축, SIEM(Security Information and Event Management) 도입 등을 통해 접속 기록을 실시간으로 모니터링하고, 비정상 행위나 위협 징후를 자동으로 탐지하여 즉각 대응할 수 있는 역량을 강화해야 한다.

개인정보보호위원회의 「개인정보의 안전성 확보조치 기준」 개정은 디지털 대전환 시대에 개인정보 보호를 위한 필수적인 진화 과정의 일부이다. 기업은 이번 개정안을 통해 개인정보 보호에 대한 인식을 재정립하고, 단순히 법적 의무 준수를 넘어 기업의 정보보호 역량을 한 단계 더 끌어올리는 계기로 삼아야 한다. 이는 단순히 법적 리스크를 회피하는 것을 넘어, 고객과의 신뢰를 구축하고 지속 가능한 비즈니스를 영위하기 위한 핵심적인 경쟁 우위가 될 것이다.

변화하는 규제 환경에 효과적으로 대응하고 개인정보 보호 역량을 강화하기 위해서는 개인정보보호법 분야의 깊이 있는 이해와 풍부한 실무 경험을 바탕으로 가지고 있는 법률전문가로부터 자문이나 실질적 솔루션 제공 도움을 받는 것이 바람직하다.

현수진 변호사

프로필 보기

02-532-3425
hyunsj@minwho.kr

법무법인 민후

MINWHO NEWS

최주선 변호사, K-CPO 컨퍼런스 참가해 '개인정보 관련 처분 사례 분석' 발표

최주선 변호사, K-CPO 컨퍼런스 참가해 '개인정보 관련 처분 사례 분석' 발표

지난 9월 23일, 개인정보전문가협회(KAPP)와 한국CPO협의회(K-CPO)가 공동 주최한 'K-CPO 컨퍼런스(K-CPO Voice)'가 서울 중구 그랜드센트럴에서 성황리에 개최되었습니다. 이번 행사는 '열린 참여, 하나 된 목소리'를 주제로 개인정보 보호책임자(CPO)들이 모여 최신 현안을 공유하고 제도 개선 방향을 논의하는 자리였습니다.

이 자리에서 법무법인 민후의 최주선 대표변호사는 '개인정보 관련 처분 사례 분석'을 주제로 발표를 진행하였습니다. 실제 처분 사례를 분석하고 실무적 시사점을 제시하여 참석자들로부터 큰 주목을 받았으며, 기업과 기관의 개인정보 보호 체계를 강화하는 데 도움이 될 실질적 가이드라인을 제공했습니다.

또한 이번 컨퍼런스에서는 개인정보 보호 정책의 흐름과 CPO의 역할, 안전한 개인정보 처리 사례 발표, 그리고 규제기관에 바라는 정책 방향에 대한 자유 토론 및 Q&A 세션이 이어져, 다양한 시각과 경험이 활발히 교류되었습니다.

행사는 많은 관심과 참여 속에 성공적으로 마무리되었으며, 디지털 전환과 AI 시대에 맞는 개인정보 보호 전략을 모색하는 의미 있는 계기가 되었습니다.

법무법인 민후는 앞으로도 최주선 대표변호사를 중심으로 기업과 기관이 직면한 개인정보보호 과제에 대해 깊이 있는 법률적 해석과 실질적 해답을 제시할 수 있도록 최선을 다할 것입니다.

MINWHO NEWS

김경환 변호사, '포장도 법적 보호 대상' 메로나 표절 분쟁 법리해석 관련 인터뷰

김경환 변호사, '포장도 법적 보호 대상' 메로나 표절 분쟁 법리해석 관련 인터뷰

빙그레가 '메로나' 포장 디자인을 둘러싼 소송 항소심에서 경쟁사 서주를 상대로 승소했습니다. 이번 판결은 단순히 아이스크림 업계를 넘어, 식품업계 전반에 퍼져 있던 포장 디자인 모방 관행에 제동을 건 사례로 주목받고 있습니다.

법원은 1심과 달리 항소심에서 소비자 조사 결과와 브랜드 주지성을 근거로 메로나 포장의 식별력을 인정했는데요. 그동안 제품 용기나 외형이 아닌 '포장 디자인'만으로는 권리 보호를 받기 어려웠던 점을 고려할 때, 이번 판결은 업계 판례로서 상징적 의미가 큽니다.

특히 소비자 설문조사가 결정적 역할을 했습니다. 다수 응답자가 '메로나' 포장만 보고 브랜드와 회사를 정확히 특정한 반면, 서주의 제품은 동일 조건에서 브랜드 및 회사명을 제대로 떠올리지 못했다는 점이 법원의 판단에 반영됐습니다.

이 판결로 인해 유사 제품 포장을 통한 소비자 혼동 유발 행위에 법적 제동이 걸릴 가능성이 커졌으며, 나아가 기업들이 포장 디자인 역시 지식재산권 보호의 중요한 대상임을 인식하고, 브랜드 가치를 지키기 위한 법적 대응에 적극적으로 나설 것으로 전망됩니다.

법무법인 민후 김경환 변호사는 '이번 판결은 포장 색상이나 구성과 같은 요소도 법이 보호하는 자산이라는 점을 확인시켜줬다'며, '지속가능한 브랜드 가치 확보를 위해 포장 디자인의 권리성을 강화하는 계기가 될 것'이라고 강조했습니다.

MINWHO NEWS

양진영 변호사, AI윤리협의체 포럼 ‘AI 정서 교감의 법적 쟁점' 발표자로 참여

양진영 변호사, AI윤리협의체 포럼 ‘AI 정서 교감의 법적 쟁점' 발표자로 참여

법무법인 민후 양진영 변호사는 서울 서초동 변호사회관에서 열린 AI윤리협의체 주최 포럼에 연사로 참여해 ‘AI와 인간의 정서적 교감이 불러올 법적·윤리적 과제’를 주제로 강연을 진행했습니다.

양 변호사는 발표에서 인공지능이 인간과 감정을 주고받는 과정에서 발생할 수 있는 오해와 의존성 문제, 개인정보 처리 이슈 등을 사례와 함께 설명하며 해외의 대응 방식을 소개했습니다. 또한 국내에서도 인공지능기본법 등 법제 정비를 통해 사회적 신뢰를 확보하고, 감정 교류형 AI의 윤리적 한계를 설정해야 한다는 점을 강조했습니다.

이번 포럼은 한국여성변호사회와 한국IT여성기업인협회의 후원으로 진행되었으며, 기술 동향 분석과 AI 감정 기능에 대한 패널 토론 등이 이어져 다양한 관점에서 논의가 이뤄졌습니다.

양진영 변호사는 법무법인 민후의 대표변호사로서, AI 윤리 및 법제도 분야의 전문성을 바탕으로 활발히 활동하고 있습니다. 이번 강연 역시 AI 시대에 예상되는 사회적·법적 쟁점을 선제적으로 검토하고, 관련 법률자문을 제공하는 과정의 일환으로서 의미를 갖습니다. 앞으로도 AI와 법제도의 균형 발전을 위해 전문적인 견해를 지속적으로 제시할 것입니다.

Business CASE

이달의 주요 업무사례

1. 계약해제로 인한 원상회복사건에서 원고 대리하여 약 10억 5천만 원 지급받는 화해권고결정 도출

2. 고소인의 이의신청으로 재수사된 상표법위반 형사고소사건에서 피의자 대리하여 불송치결정 도출

3. 상품형태 모방으로 인한 부정경쟁방지법 위반 사건에서 피고소인을 대리하여 불기소(혐의 없음) 처분 이끌어 승소

4. 채무불이행 및 계약취소로 인한 계약금반환청구 등 사건에서 원고를 대리해 계약금 전액 반환 및 손해배상금 약 3,500여만 원 지급 판결 승소

5. 계약해제로 인한 용역대금반환소송에서 피고를 대리하여 청구금액의 약 70% 감액 조정 결정 도출

6. 제품 디자인 유사성으로 인한 저작권침해행위·부정경쟁행위 내용증명 발송, 상대방 회신서 검토 및 법적 대응 법률자문

7. 스타트업 대상 투자자문을 수행하는 기업과의 투자대행계약서 초안 검토 및 조항 보완 자문

8. AI 데이터 수집·가공 기업의 글로벌 파트너십 계약서 검토 법률자문

9. 채용 플랫폼 구직자 대상 알림 톡·이메일 발송 시 광고성 정보 판단 기준 및 수신 동의 절차 등 검토 법률자문

10. 온라인 채용·구인구직 플랫폼 운영 기업에 직무발명 보상규정 및 보상 합의서 작성 법률자문

법무법인 민후

서울특별시 강남구 테헤란로 134, 포스코 타워 역삼 11층

Tel. +82-2-532-3483 **Fax.** +82-2-532-3486

www.minwho.kr

[변호사 소개 바로가기] [주요 업무사례 바로가기]

[전화 상담 바로가기] [카톡 상담 바로가기] [홈페이지 상담 바로가기] [이메일 상담 바로가기]

본 뉴스레터의 내용 또는 기타 법률 문의가 필요하신 경우
법무법인 민후로 연락주시면 담당 변호사님의 답변을 받으실 수 있습니다.