

개인정보보호법 개정안 〈9월 15일〉 시행 확정

- ✓ 개인정보 보호관련 중대과실 발생시
〈최대 전체 매출액 3% 과징금〉
- ✓ 공공, 기업, 금융 마이데이터 확산
〈개인정보 전송요구권〉
- ✓ 개인정보 사적 이용 시
〈5년 이하 징역 또는 5천만원 이하 벌금〉

개정 01.

위반행위시

최대 전체 매출액 3% 과징금 부과

개인정보 보호관련 중대과실 발생시

최대 매출액 3% 과징금 부과

단, 전체 매출액에서 위반행위 관련 없는 매출은 제외

[상세한 소명자료 미제출시 전체 매출 과징금 부과 가능]

개인정보보호법 제64조의2 (과징금의 부과) 신설



- ✓ 단, 매출액이 없거나 산정이 곤란한 경우
20억원을 초과하지 않는 범위 내에서 확정

개정 02.

개인정보 전송요구권 신설

공공·민간·금융 전 분야 마이데이터 확산

신용정보법, 전자정부법에만 규정된

‘개인정보 전송요구권’ 신설

정보주체가 개인정보 전송사업자에게 본인의 개인정보를
본인·개인정보관리기관 등에 전송 요구할 수 있음

전송대상에서 제외되는 개인정보 범위는 ‘시행령’에 규정

제35조의2 (개인정보의 전송요구) 신설



- ✓ 개인정보전송(마이데이터) 사업을 계획하고 있을 경우
개인정보보호법 시행에 맞추어 사전대비 필요

개정 03.

개인정보 사적 이용 시

5년 이하 징역 또는 5천만원 이하 벌금

‘개인정보를 처리하거나 처리하였던 자’가 자신의 권한을
초과하여 타인의 개인정보를 <이용>할 경우 처벌
수험생 응시원서/민원인 개인정보를 취득하여
사적으로 연락을 취한 수능감독관/경찰관 판례 영향

제59조 제3호 (금지행위) 일부개정



- ✓ 개인정보를 훼손, 멸실, 변경, 위조, 유출하는 경우 뿐만 아니라 <이용>하는 경우에도 처벌
- ✓ 공익근무요원, 경찰관, 시험감독관 등 사례에서 보여졌던 사적 이용행위에 관하여 처벌 가능
- ✓ **사고예방 및 기업/기관 평판유지를 위한 관리적 보호조치 강화**

개정 04.

손해배상한도 손해액 기준

최대 3배에서 5배로 기준 상향

개인정보처리자의 고의 또는 중대 과실로 인하여
개인정보가 분실·도난·유출·위조·변조 또는 훼손되어
정보주체 손해가 발생한 때,
법원은 손해액의 <5배>를 넘지 않는 범위에서 손해배상액 산정
제39조 제3항 (손해배상책임) 일부개정



- ✓ 기존 배상처리 금액기준 약 1.6배 증가
- ✓ 단, 개인정보처리자가
고의 또는 중대한 과실이 없음을 증명한 경우 해당되지 않음

개정 05.

침해사고 사전예방 목적

사전 실태점검 시행

위반사항 및 관련 혐의(민원)가 없어도
개인정보 침해사고 발생 위험이 높고,
유출 시 파장이 클 경우
사전 개인정보보호 실태점검 시행

제63조의2 (사전 실태점검) 신설



- ✓ 사전 점검 시 위반사항 발생하더라도 과태료, 과징금 부과없음
- ✓ 10일 내에 시정권고 수락여부 통지 및 개선
- ✓ 개인정보 유출사고 예방 및 시정권고사항 개선을 위한
기술적 관리적 보호조치 필요

개정 06.

자동화 결정에 대한 정보주체 권리 신설

인공지능 기술을 포함한 완전히 자동화된 시스템으로
개인정보를 처리할 때 정보주체 권리/의무에
중대한 영향을 미칠 경우 해당 결정을 거부할 수 있음

제37조의2 (자동화된 결정에 대한 정보주체의 권리 등) 신설



- ✓ 자동화 결정이 1) 정보주체 동의를 받은 경우 2) 법률에 특별규정이 있거나 법령의무 준수를 위해 불가피한 경우 3) 정보주체와 계약체결을 위해 불가피하게 필요한 경우 제외
- ✓ 자동화 거부 시 인적개입을 통해 개인정보 처리
- ✓ 자동화 결정 거부 절차/방법, 필요조치, 개인정보 처리방식 공개 등 세부사항은 대통령령으로 결정

개정 07. 개인정보 국외이전, 중지명령권 신설

개인정보가 이전되는 국가 또는 국제기구가 개인정보를
적정하게 보호하고 있지 않다는

명백한 사유(법 위반 등)가 있을 경우

‘해당기업(개인정보처리자)’에게 전송이동 중지 요구가능

제28조의9 (개인정보의 국외이전 중지명령) 신설



- ✓ 법 위반 등 개인정보보호에 있어 중지명령권 발동 확률이 높은 곳으로 개인정보를 이전하는 경우 대응책을 마련해야 함
- ✓ EU (21'말 적정성 결정), 영국(22' 11월 적정성 결정 입법절차 완료), CBPRs(APEC 개인정보보호 인증제도: 한국, 미국, 멕시코, 일본, 캐나다, 싱가포르, 호주, 대만, 필리핀) 회원국

이외 개정사항

정부안 및 의원발의안 21개 안건 통합 상정

개인정보 영향평가	영향평가를 실시하지 않거나 결과를 보호위에 제출하지 않은 경우, 3천만원 이하 과태료 부과
공공기관 개인정보 보호수준 평가	중앙행정기관, 소속기관, 지자체 대상 연1회 개인정보보호 정책 업무 수행 및 법규 준수여부 등 평가 결과는 인터넷 홈페이지에 게시
개인정보 목적 외 이용제공제한	계약체결/이행을 위해 필요한 경우 수집가능
영상정보 규제	이동형 CCTV 규제 신설, 자율주행/드론 등 신기술 침해대응 [공개된 장소에서 업무목적의 사람/사물 촬영 금지, 촬영 시 촬영사실 표시]
민감정보 고지의무	민감정보 사전고지 의무 및 비공개 방법 신설
가명정보 특례정비	가명정보 파기시 파기기록 작성하여 3년 이상 보관
분쟁조정	분쟁조정 통지를 받은 경우, 특별사유가 없으면 참여해야 하는 대상에 기존 공공기관에서 모든 개인정보처리자까지 포함
개인정보보호의 날 지정	9월 30일 지정

출처: 의안정보시스템 개인정보보호법 일부개정법률안(대안) - 2023.02.27 원안가결
https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_M2G2Z1U1I2C3V1E3N4W8K5I4J2L5W6

개인정보보호를 위한 주요 기술적 보호조치

항목	내용	솔루션 예시
개인정보 파기	PC, 서버, DBMS, 스마트폰에 저장된 고객 개인정보 데이터 파일 자동화된 식별 및 파기 (일정기간 활용 후 삭제 혹은 암호화)	Privacy-i Server-i DB암호화 솔루션
개인정보 유출 통제	USB, 출력물, 인터넷 파일 전송을 통한 개인정보 유출통제 단말기 반출입을 통한 유출통제	Endpoint DLP, Network DLP외
개인정보 처리 시스템 접속기록관리	개인정보 처리 시스템 정보 조회기록 (누구의 정보를 가져갔는지도 기록) 1. DBMS 직접 조회 (DB query와 결과값 기록) 2. 터미널 서비스(Telnet/SSH, FTP/SFTP 접속, 윈도우 터미널) 접속기록 3. 웹애플리케이션을 통한 개인정보 조회 기록	DB-i 웹로그 관리 솔루션
개인정보 암호화 보관 및 전송	DBMS, PC(태블릿PC, 스마트폰), 서버에 보관된 개인정보 암호화 보관 및 외부 통신 전송 암호화	Privacy-i Server-i DB암호화 솔루션 HTTPS 등 암호화통신
개인정보 처리 시스템 권한/접근통제	개인정보 처리 시스템 비인가자 접속차단 권한 부여 기록관리	DB-i
망분리	개인정보 처리시스템에 접근권한을 가진 단말은 망분리(논리적, 물리적)	논리적 망분리 (VD-i 외)
악성코드 통제	관리용 단말에 대한 악성코드 차단 조치 PC, 서버에 대한 취약점 점검	Privacy-i EDR 안티바이러스

체계적인 기술적 관리적 보호조치 방안구축은

소만사 프라이버시 컨설팅을 통해 구현하실 수 있습니다

consulting@somansa.com