2023.09.15 시행!
개인정보보호법 고시
〈개인정보의 안전성 확보조치 기준〉
개정안 행정예고

- ✓ 이용자 개인정보를 보유한 기업/기관은
  〈고유식별정보, 신용카드, 계좌번호 암호화 저장〉
- ✓ 출력파일 내 민감정보, 고유식별정보 포함시
  〈인쇄자, 인쇄일시 기록〉
- ✓ 개인정보처리시스템 접속자 접속기록
  〈3개월 이상 보관·관리〉
- ✓ 공공시스템 접근계정 발급시
  〈인사정보에 등록된 자만 발급 허용〉

01. 개정 및 강화

정보통신서비스 이용자 개인정보 보유 기업·기관은 고유식별정보, 〈신용카드, 계좌번호〉 암호화 저장

정보통신서비스를 이용하는 **'이용자'의 개인정보를 보유한 민간기업**은 **내부망/DMZ 여부와는 상관없이 7개 개인정보 패턴을 암호화 저장**해야 함

제7조 (개인정보의 암호화) ② 일부개정

- ✓ 망법고시 제6조 (개인정보 암호화)가 개보법 고시로 이관
- ✓ 다음 이용자 개인정보는 안전한 암호 알고리즘으로 암호화 저장

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

02. 신설 및 강화

출력파일 내 민감정보, 고유식별정보 포함시 〈인쇄자, 인쇄일시〉 기록

민감정보/고유식별정보를 관리하는 공공기관 및
5만명 이상 정보주체의 민감정보를 보유한 기업/기관은
출력파일 내 민감정보, 고유식별정보 포함시 종이 인쇄물
안전관리를 위해 **인쇄자, 인쇄일시 등 기록**

제13조 (출력복사시 안전조치) ③ 신설

- ✓ 망법고시 제9조 (출력복사시 보호조치)가 개보법 고시로 이관
- ✓ **엔드포인트 DLP 출력물 통제 : 인쇄자 정보 (부서, 이름, 직급 등), 인쇄 일시, 워터마킹 및 출력기록 로그저장**

03. 조항 신설

개인정보처리시스템 접속자 접속기록 〈3개월 이상 보관·관리〉

단, 기존고시와 동일하게

- ✓ **개인정보취급자 접속기록은 1년 이상** 보관·관리
- ✓ **5만명 이상 정보주체 개인정보 보유시스템 사업자, 고유식별정보 또는 민감정보 개인정보 보유시스템 사업자 기간통신사업자는 2년 이상** 보관 및 관리

제8조 (접속기록의 보관 및 점검) 일부조항 신설

- ✓ 개인정보처리시스템 접속자 접속기록에 대한 상세내용은 9월 내 발간되는 '고시해설서'에서 파악가능
- ✓ **DB 접근제어가 기록하는 접속정보: 접속자(부서, 이름, 직급, ID 등), 접속일시, 접속지 정보, 처리한 정보주체정보, 수행업무 등**

04. 신설 및 강화

공공시스템 접근계정 발급시 〈인사정보에 등록된 자〉만 발급 허용

정당한 권한을 가진 접속자에게만 접근을 허용하고
오남용을 방지하기 위해

- ✓ **인사정보에 등록된 자에게만 계정 발급**
- ✓ **개인정보보호 교육 및 보안서약서 작성 필수**
- ✓ **접근권한 부여, 변경, 말소내역 연2회 이상 점검**

제17조 (공공시스템운영기관의 접근권한 관리) 신설

- ✓ 'N번방', '박사방' 불법개인정보 조회사건
  (접근권한 없는 사회복무요원에게 행정정보 조회시스템 계정공유) 영향
- ✓ **공공시스템 접속자 접속기록은 자동화 방식으로 분석 수행**
- ✓ **개인정보 유출, 오남용 시도가 탐지될 경우 반드시 사유 소명**

이외 개정사항

조항	키워드	개정내용
제6조 접근 통제	완화 개인정보 처리시스템 외부접속방안	② 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하는 경우 **안전한 인증수단 적용**
	완화 망차단 조치	⑥ 개인정보 처리시스템 접근, 개인정보 다운로드/파기 권한있는 개인정보 취급자 컴퓨터 등에 **인터넷망 차단 조치 구축.** **클라우드컴퓨팅 서비스 이용시 해당 서비스 접속 외 인터넷 연결차단.**
제7조 개인 정보 암호화	대동소이 정보주체 개인정보 내부망/DMZ 저장	③ 1. 인터넷망 구간, 인터넷망 구간 – 내부망 중간지점(DMZ)에 고유식별정보 저장시 암호화 2. 정보주체의 고유식별정보 내부망 저장시 다음 기준에 따라 암호화 가. 영향평가 결과 나. 암호화 미적용시 위험도 분석 결과
	대동소이 내부망 전송시 암호화	④ **내부망 전송시**에도 고유식별정보, 비밀번호, 생체인식정보는 안전한 암호화 알고리즘으로 암호화
	대동소이 인터넷 전송시 암호화	④ 개인정보를 **인터넷망 구간**으로 송수신하는 경우 안전한 알고리즘으로 암호화
	강화 PC 저장시 암호화	⑤ **이용자 개인정보 및 이외 정보주체의 고유식별정보/생체인식정보** 개인정보 취급자의 **컴퓨터, 모바일기기, 보조저장매체에 저장시** 상용암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장
	강화 USB 저장시 암호화	
	완화 개인정보 암호화 및 보관계획 수립	⑥ **(10만명 개인정보처리) 대기업/중견기업/공공기관 또는 (100만명 개인정보처리) 중소기업/단체는** 안전한 암호키 생성, 이용, 보관, 배포, 파기 절차 수립

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 암호화 통신
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

SOMANSA