개인정보보호법 고시
개인정보의 안전성 확보조치 기준
개정 행정예고

25.7.21 보호위, “개인정보의 안전성 확보조치 기준” 일부개정고시안 행정예고

3대 변화 요약

1. 인터넷 망분리 예외대상 규정

DB DLP, 서버 DLP, 엔드포인트 DLP 등
정보유출 위험을 감소할 수 있는 **보호조치를 개인정보처리자 PC에 구축**한 경우
→ 생성형AI서비스, 클라우드 서비스 활용 가능

2. 오픈마켓 입점 판매자 처리시스템 접속대상에 포함

처리시스템 접속 시
안전한 인증수단으로 접속, **접속기록 보관/관리**
→ 접속기록 책임 추적성 확보

3. 개인정보처리시스템 접속기록 점검규정 자율화

월1회 규정에서 개인정보규모, 유형,
내부지침에 따라 **자율적으로 수립 및 운영.**
→ 추후 조치 미흡으로 유출사고 발생시 기관책임

1. 신설 및 보호조치 강화

DB DLP, 서버 DLP, 엔드포인트 DLP 등 정보유출 위험을 감소할 수 있는 **보호조치를 구축**한 **개인정보처리자의 PC**에는 **인터넷 망분리 예외 처리** 가능 **생성형AI, 클라우드 서비스 도입 및 활용**가능

6조의2 인터넷망의 차단조치 등

① 이용자 수가 일일평균 100만명 이상인 개인정보처리자는
다음 각 호의 어느 하나에 해당하는 개인정보취급자의 컴퓨터 등에 대해
인터넷망 차단 조치를 하여야 함.
1. 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자
2. 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있는 개인정보취급자

② 개인정보처리자는 내부 관리계획에서 정한 위험 분석 결과가
다음 각 호의 어느 하나에 해당하는 경우에는
인터넷망 차단 조치를 하지 아니할 수 있음.
다만, 법 제23조에 따른 민감정보 또는 제7조제1항·제2항에 따른
개인정보를 다운로드 또는 파기할 수 있는
개인정보취급자의 컴퓨터 등에 대해서는 그러하지 아니함.
1. 위험 분석 결과 확인된 위험이 현저히 낮은 경우
2. 위험 분석 결과 확인된 위험을 감소시킬 수 있는 보호조치를 적용한 경우.
이 경우 개인정보처리자는 **[별표]에 따른 예시**를 고려하여야 함.

〈신설〉 별표

위험을 감소시킬 수 있는 보호조치 예시

(제6조의2 관련)

구분	보호조치 예시	기술적 보호조치
개인정보 파일을 다운로드 할 수 있는 개인정보 취급자의 컴퓨터 등	개인정보처리시스템 접속 시 안전한 인증수단 적용	2팩터 인증
	개인정보 파일 저장 시 안전한 암호 알고리즘으로 암호화	엔드포인트 DLP 서버 DLP 파일 암호화
	개인정보 다운로드 건수 제한	DB DLP
	개인정보 다운로드 권한을 가진 개인정보취급자 최소화	DB 접근제어 (계정관리)
	개인정보 출력시 마스킹, 안심번호 등 표시제한 조치 적용	Endpoint DLP
개인정보 파일을 파기 할 수 있는 개인정보 취급자의 컴퓨터 등	개인정보 파기 권한을 가진 개인정보취급자 최소화	DB 접근제어 (계정관리)
	개인정보 파기시 관리자 등으로부터 별도 승인을 받도록 설정	서버 DLP

※ “예시”는 개인정보처리자가 개인정보에 대한 접근을 통제하기 위해 필요한 조치를 마련하는 과정에서 ‘필요한 조치’에 해당하는지를 판단할 때 적용해야 하는 안전조치 사례로, 실제 사례에서는 구체적 사실관계에 따라 필요한 부분을 선별적으로 적용할 수 있음

2. 적용대상 확대

오픈마켓 입점 판매자
처리시스템 접속대상에 포함

처리시스템 접속 시
안전한 인증수단으로 접속, 접속기록 보관/관리
접속기록 책임 추적성 확보

5조 접근권한의 관리

① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을
~~**개인정보취급자에게만**~~ 업무 수행에 필요한
최소한의 범위로 차등 부여하여야 힘

⑥ 개인정보처리자는 정당한 권한을 가진 **자가**
~~**개인정보취급자 또는 정보주체만이**~~
개인정보처리시스템에 접근할 수 있도록 일정 횟수 이상 인증에 실패한 경우
개인정보처리 시스템에 대한 접근을 제한하는 등 필요한 조치를 하여야 함

2. 적용대상 확대

오픈마켓 입점 판매자 처리시스템 접속대상에 포함

처리시스템 접속 시
안전한 인증수단으로 접속, 접속기록 보관/관리
접속기록 책임 추적성 확보

6조 접근통제

② 개인정보처리자는 ~~개인정보취급자~~
개인정보처리시스템에 대한 정당한 접근권한을 가진 자(정보주체는 제외)가
정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우
인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 함.
이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우
가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있음.

8조 접속기록의 보관 및 점검

① 개인정보처리자는 ~~개인정보취급자의 개인정보처리시스템에 대한~~
개인정보처리시스템에 접속한 자(정보주체는 제외)의 접속기록을
1년 이상 보관·관리해야 한다.
다만, 다음 각 호의 어느 하나에 해당하는 경우 2년 이상 보관·관리해야 함.

1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템
2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템
3. 개인정보처리자로서 「전기통신사업법」에 따라 등록, 신고한 기간통신사업자

3. 자율규제

개인정보처리시스템 접속기록 점검규정 자율화

월1회 규정에서

개인정보규모, 유형, 내부지침에 따라

기업/기관이 자율적으로 수립 및 운영

조치 미흡으로 유출사고 발생시 기업/기관책임

8조 접속기록의 보관 및 점검

② 개인정보처리자는 개인정보의
오 · 남용, 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손 등에
대응하기 위하여 개인정보처리시스템의
~~접속기록 등을 월 1회 이상 점검하여야 함.~~
~~특히 개인정보의 다운로드가 확인된 경우에는 내부 관리계획 등으로~~
~~정하는 바에 따라 그 사유를 반드시 확인하여야 함.~~

접속기록 및 개인정보 다운로드 상황을 확인하고
점검 주기·방법·사후조치절차 등을
내부 관리계획으로 정하고 이행 하여야 함.

주요 개정사항 요약

조항	2025.07.21 행정예고 '개인정보의 안전성 확보조치 기준'	기술적 보호조치
5조 접근 권한의 관리	① 개인정보처리자는 개인정보처리시스템에 대한 **접근 권한을 업무 수행에 필요한 최소한의 범위로 차등 부여**하여야 함.	DB DLP 서버 DLP DB 접근제어
	⑥ 개인정보처리자는 **정당한 권한을 가진 자**가 개인정보처리시스템에 접근할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리 시스템에 대한 접근을 제한하는 등 필요한 조치를 하여야 함.	DB접근제어
6조 접근통제	② 개인정보처리자는 **개인정보처리시스템에 정당한 접근권한을 가진 자(정보주체 제외)**가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 함. 다만, 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있음.	2팩터 인증 (인증서, 일회용 비밀번호 등)
6조의2 인터넷 망의 차단조치 등	**① 전년도 말 기준 직전 3개월간 그 개인정보가 저장 · 관리되고 있는 이용자 수가 일일평균 100만명 이상인 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 개인정보취급자의 컴퓨터 등에 대해 인터넷망 차단 조치를 하여야 함.** **1. 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자** **2. 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있는 개인정보취급자**	논리적 망분리 (클라우드 PC) 물리적 망분리
	② 1항 2호에도 불구하고 개인정보처리자는 내부 관리계획에서 정한 위험분석 결과가 다음 각 호 어느 하나에 해당하는 경우, 인터넷망 차단조치를 하지 아니할 수 있음. 다만, 법 23조에 따른 민감정보 또는 7조 1항·2항에 따른 개인정보를 다운로드 또는 파기할 수 있는 개인정보취급자의 컴퓨터 등에 대해서는 그러하지 아니함. **1. 위험 분석 결과 확인된 위험이 현저히 낮은 경우** **2. 위험 분석 결과 확인된 위험을 감소시킬 수 있는 보호조치를 적용한 경우. 이 경우 개인정보처리자는 [별표]에 따른 예시를 고려하여야 한다**	2팩터 인증 파일 암호화 DB 접근제어 DB DLP 엔드포인트 DLP 서버 DLP 등
8조 접속 기록의 보관 및 점검	① 개인정보처리자는 **개인정보처리시스템에 접속한 자(정보주체 제외)**의 접속기록을 1년 이상 보관·관리해야 함. 다만, 다음 각 호의 어느 하나에 해당하는 경우 2년 이상 보관·관리. 1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템 2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템 3. 개인정보처리자로서 「전기통신사업법」에 따라 등록, 신고한 기간통신사업자	DB접근제어 (개인정보 접속기록관리) APP서버 로그관리
	② 개인정보처리자는 개인정보의 오남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 및 **개인정보 다운로드 상황을 확인하고 점검 하는 주기·방법·사후조치절차 등을 내부 관리계획으로 정하고 이행 하여야 함.**	

SOMANSA

참고자료

[개인정보보호위원회]
「개인정보의 안전성 확보조치 기준」 일부개정고시안 행정예고
https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS061&mCode=C010010000&nttId=11369#LINK

[개인정보보호위원회]
개인정보처리자 대상 일률적인 인터넷망 차단조치 규제를 개선한다
https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=11364

[소만사 프라이버시 리포트]
‘개인정보의 안전성 확보조치 기준’
개정 행정예고
기존 고시 대비 변경사항 전체 보기

체계적인 기술적 관리적 보호조치 방안구축은
소만사 프라이버시 컨설팅을 통해
구현하실 수 있습니다

consulting@somansa.com

SOMANSA