

개인정보의 안전성 확보조치 기준 개정(안), 개인정보처리시스템의 접속기록에대한 관리기준 강화

행정안전부공고
제2019-81호 보기

1. 접속기록의 기록항목 구체화

(신설) 접속기록을 육하원칙에 따라 구체적으로 명시,
특히 “누구의” 개인정보를 조회했는지 기록 필요

필수기록항목	구분	설명
접속자 ID	Who (누가)	개인정보취급자 식별정보
접속자 IP		접속자 PC, 단말기의 정보 등
날짜 및 시간	When (언제)	접속일시
수행업무	Whose (누구의)	정보주체에 대한 접속기록 (누구의 정보에 접속했는지)
	How (어떻게)	열람/저장*/수정/삭제/출력 등

특정인의 개인정보
침해발생 시 추적을 위해
‘누구의’ 개인정보를
조회했는지 기록 필요**

* 저장 시 사유를 반드시 기록해야함

**2019 고시 개정 방향’ 정부기관 발표 내용 발췌

2. 접속기록 보관기간 최소 1년 이상 보관

접속기록 보관기간을 중요도에 따라 차등적 연장 검토

기존 고시 제8조 2항

개인정보처리시스템 접속기록
6개월 이상 보관 및 관리

(문제점)

6개월이 경과한 접속기록 삭제가 관례가 됨

개인정보 유출사고가 6개월 이후에 발견되면
접속기록이 없어 유출원인을 추적하기 어려움

접속기록 보관기간 변경 내용

- ① 개인정보처리시스템 접속기록 1년 이상 보관
- ② 5만명 이상의 개인정보를 처리하거나,
고유식별정보 또는 민감정보를 처리하는
시스템은 2년이상 보관
- ③ [2022년 부터] 생성되는 접속기록은 3년 이상,
[2025년 부터] 생성되는 접속기록은 5년 이상
보관

3. 접속기록 점검 주기 단축

접속기록 점검을 반기별 1회 이상에서 월 1회 이상으로 단축

접속기록 점검 주기 변경	
변경 항목	① 접속기록을 (반기별 1회에서) 월 1회 이상 점검으로 변경
신설 항목	① 내부 관리계획 이행실태 점검에 접속기록에 관한 사항 포함
	② 개인정보를 다운로드한 경우 그 사유를 반드시 확인*

*2018년도 모 기관의 사례처럼 개인정보처리시스템에서 대량의 개인정보가 다운로드/유출된 사고가 발생했음에도 불구하고 이와 관련된 접속기록이 남지 않아, 누구의 개인정보가 다운로드되어 유출되었는지 추적이 불가능하였음

개인정보 보호법 고시 개정(안) 대응방안

개인정보처리시스템 접속경로	접속기록 대응방안	기술적 보호조치
쿼리툴 접속	쿼리툴 결과값 저장(Sample 저장)	DB접속기록, DB DLP
웹 Apps 접속	개인정보처리시스템에서 조회한 개인정보 기록	웹접속기록 관리
	다운로드된 개인정보 원본 기록	Network DLP

(주)소만사 서울시 영등포구 영신로 202 knk디지털타워 9층
TEL 02-2636-8300 | FAX 02-2636-8181 | Email privacy@somansa.com
copyright (C) 1997-2019 SOMANSA ALL RIGHTS RESERVED.

본 메일은 회원님께서 수신동의를 하셨기에 발송되었습니다
뉴스레터 수신을 더 이상 원하지 않으실 경우 **[수신거부]**를 클릭해주세요.
수신거부 클릭이 안 되실 경우 privacy@somansa.com으로 수신거부의사를 밝혀주시면 신속하게 처리해드리겠습니다.