소만사 보안성 지속서비스 Annual Report

프라이버시 리포트

(2015.05~2016.06)

목차

관련법 개 인정보보호법 정 보통신망법 전 자금융거래법 국 민건강보험법

1.개인정보보호법 (적용대상: ALL)

2. 정보통신망법 (적용대상 : 정보통신서비스 제공자)

3. PIMS인증 (적용대상 : 공공기관 · 대기업 · 중소기업 · 소상공인)

4. 전자금융감독규정 (적용대상 : 금융회사 · 전자금융업자)

5. 의료기관 · 약국의 개인정보보호 변화 (적용대상 : 의료기관 · 약국)

01

개인정보보호법

(적용대상 : All)

2016년 개정, 개인정보보호법 변화

개인정보보호법 원문보기 | 시행령 원문보기 | 이전 Report 보기

① 〈민감정보〉 대상으로 강화

민감정보가
분실 도난 유출
위조 변조 훼손
되지 않도록
〈개인정보의 안전성 확보조치 기준〉 적용
법 23조 ②항

민감정보에
〈개인정보의 안전성 확보조치 기준〉
미조치로 유출시
형사처벌
몰수추징
손해배상

이전 Report 보기

② 〈고유식별정보〉 대상으로 강화

~2017.01.01까지
(저장된 주민등록번호 명수가)
100만명 미만일 경우
내부망 주민등록번호
암호화완료

~2018.01.01까지
(저장된 주민등록번호 명수가)
100만명 이상일 경우
내부망 주민등록번호
암호화완료

개인정보보호법고시
〈개인정보의 안전성 확보조치 기준〉 강화

2년에 1회 〈고유식별정보〉에
〈개인정보의 안전성 확보조치 기준〉
적용여부를
행자부(or KISA)에 온라인 or 서면 제출

③ 〈PIMS 인증 및 PIA〉 대상으로 강화

PIMS인증
〈관리적기술적 물리적보호대책〉 포함
인증기준 고시예정
시행령 34조의4

PIA
평가항목에 기술적보호조치 20개 신설
(2015.12.31 영향평가에 대한 고시)

이전 Report 보기

고유식별정보에 〈개인정보의 안전성 확보조치 기준〉 미조치로 유출시 형사처벌 몰수추징 손해배상

주민등록번호를 수집할 수 있는 법령범위를
법률/대통령령/국회규칙/대법원규칙/헌법재판소규칙/
중앙선관위규칙 및 감사원규칙으로 한정
법 24조의2 ①항 1호

이전 Report 보기

④ 그 외 규정들

〈개인정보보호위원회〉 강화

전문위원회 위원 증원 (5명→10명)
법 5조

관련기관에 정책/제도/법령
개선 권고 가능
법 9조의2

중앙행정기관의 개인정보
침해요인 평가절차규정
법 9조의3

CPO 관련규정 명확화

임원
(없는 경우 개인정보 처리부서의 장)
법 32조

개인정보처리방침에 CPO 성명 추가
(개인정보부서의 명칭, 연락처, 인터넷접속,
정보파일 등 개인정보 자동수집장치 내역을
개인정보처리방침에 추가)
법 30조 ①항

개인정보를 제공받은
경우 3개월이내에
정보주체에게
제공받았다는 사실을
1:1로 고지

2016년 개정, 개인정보보호법 변화 연대표

발송일
2016. 05

2016년 5월 공청회실시→의견수렴→8월 확정예정

개인정보보호법고시

〈개인정보의 안전성 확보조치 기준〉개정안

원문보기

적용대상자의 변화 — 3개 유형으로 분류, 차별적으로 법 적용

유형3 강화 (56개 적용)		유형2 표준 (49개 적용)		유형1 완화 (28개 적용)
10만명 이상 개인정보를 보유한 공공기관, 대기업, 중견기업	100만명 이상 개인정보를 보유한 중소기업	10만명 미만 개인정보를 보유한 공공기관, 대기업, 중견기업	100만명 미만 개인정보를 보유한 중소기업	1만명 미만 개인정보를 보유한 소상공인 단체, 개인

\+ \+ \+

수탁자 (위탁자의 유형에 따라 동일한 안전조치 기준 적용)

기술적 보호조치 신설 및 추가

개인정보처리시스템	계정 오입력시 접근제한	5조	⑥ ID, PW 일정횟수 이상 잘못 입력시 접근제한
	불법유출시도 대응		① 2. 접속 IP등을 분석, 불법유출시도 탐지 및 대응
	공인인증서	6조	② 외부접속시 안전한 접속수단으로 VPN, 전용선, 공인인증서
	관리용단말기		④ 관리용단말기에 네트워크를 통한 유출방지조치
	시간경과시 접속차단		⑥ 일정시간 특정업무처리를 하지 않을 경우 자동 접속차단
	연1회 취약점점검→ 보완		⑨ 연1회 이상 취약점을 점검, 필요한 보완조치를 하여야 한다
	접속기록점검으로 취약점발견→즉시 보완		⑩ 접속기록점검결과 취약점발견시 즉시 보완조치
	관리용단말기 보안조치	10조	1. 비인가자가 임의조작 못하도록 조치 2. 본래 목적외로 사용되지 않도록 조치 3. 악성프로그램 감염방지등을 위한 보안조치 적용
	화재, 홍수, 단전시 재해 재난 대비	12조	① 위기대응매뉴얼 등 대응절차마련, 정기점검 ② 백업 및 복구계획마련
암호키 절차 수립		7조	⑥ 암호키 생성, 이용, 보관, 배포 및 파기 절차 수립 시행

내부관리계획 강화

반드시 포함해야 하는 항목이 기존 6개→15개로 증가

3개 유형별로 차별적 적용

CPO가 연1회 이상 내부관리계획 이행실태 점검

고시 4조 ④항

〈개인정보의 안전성 확보조치 기준〉 고시 상세규정보기

~~TEXT~~(취소선) : 삭제된 규정 파란색 텍스트 : 신설 or 추가된 규정

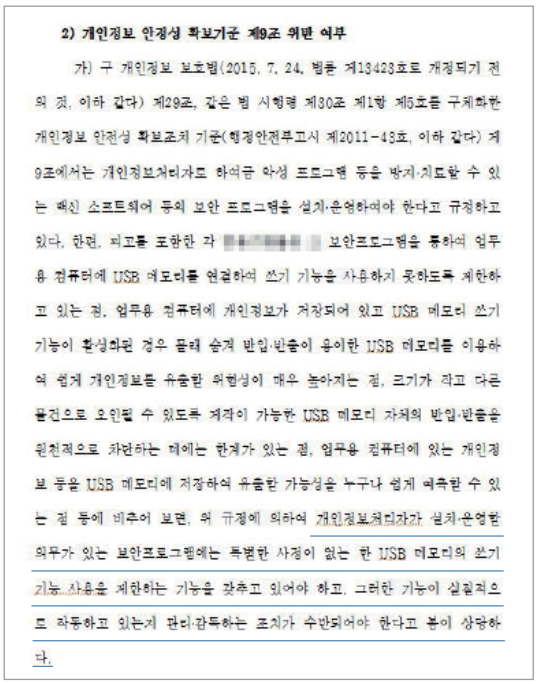
조	내용	유형별 적용여부			보호조치
		유형3	유형2	유형1	
1조 목적	(법 24조③항 · 29조, 시행령 21 · 30조에 따라) 개인정보가 분실,도난,유출, 위조, 변조,훼손되지 않도록 (개인정보처리자가 지켜야하는) 안전성확보기준을 정함	–	–	–	
2조 정의	〈총 20개의 용어정의〉 정보주체, 개인정보파일, 개인정보처리자, 대기업, 중견기업, 중소기업, 소상공인,개인정보보호책임자, 개인정보취급자, 개인정보처리시스템, 위험도분석, 비밀번호, 정보통신망, 공개된 무선망. 모바일기기, 바이오정보,보조저장매체, 내부망, ~~내부관리계획~~, 접속기록, 관리용단말기 대기업 (→독점규제 및 공정거래에 관한 ~~법률 14조~~에 따라 공정위가 지정한 기업) 중견기업 (→중견기업 성장촉진 및 경쟁력강화에 따른 특별법 2조 해당기업) 중소기업 (→중소기업 기본법 2조 및 시행령에 따른 기업) 내부망 (→물리적망분리, 접근통제시스템등에 의해 인터넷구간에서의 접근이 통제 or 차단되는 구간) 관리용단말기 (→개인정보처리시스템의 관리, 운영, 개발, 보안등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기)	–	–	–	
3조 적용	**개인정보처리자 유형 및 개인정보보유량에 따른 안전조치기준을 적용해야한다. 이 경우 개인정보처리자가 어느 유형에 해당하는지 입증책임은 개인정보처리자가 부담한다**	–	–	–	
4조 내부관리 계획의 수립/ 시행	① 내부관리계획에 포함되는 사항	–	–	–	[컨설팅]
	1. 개인정보보호책임자지정	○	○	X	
	2. 개인정보보호책임자 및 취급자의 역할 · 책임	○	○	X	
	3. 개인정보취급자교육	○	○	X	
	4. 접근권한의관리에 관한 사항	○	○	X	
	5. 접근통제에 관한 사항	○	○	X	
	6. 개인정보의 암호화 조치에 관한 사항	○	○	X	
	7. 접속기록 보관 및 점검에 관한 사항	○	○	X	
	8. 악성프로그램 등 방지에 관한 사항	○	○	X	
	9. 물리적안전조치에 관한 사항	○	○	X	
	10. 개인정보보호조직에 관한 구성 및 운영에 관한 사항	○	○	X	
	11. 개인정보유출사고 대응계획 수립 시행에 관한 사항	○	X	X	
	12. 위험도 분석 및 대응방안 마련	○	X	X	
	13. 재해 및 재난대비 개인정보처리시스템의 물리적 안전조치에 관한 사항	○	X	X	
	14. 개인정보처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 대한 사항	○	X	X	
	15. 그 밖에 필요한 사항	○	○	X	
	② 유형1은 수립제외. 유형2는 11~14 적용제외	–	–	–	
	③ ①에 변화가 생길시, 즉시 수정 및 시행 후 이력관리	○	○	X	
	④ 개인정보보호책임자는 연1회 이상으로 내부관리계획의 이행실태 점검 관리	○	○	X	

조	내용	유형별 적용여부			보호조치
		유형3	유형2	유형1	
5조 개인정보 처리 시스템 접근권한 관리	① 최소한의 범위로 개인정보처리시스템 접근권한 차등부여	○	○	X	접근통제솔루션 [DB] DB-i [WAS] WAS-i [SAP] App-i
	② 인사이동시 개인정보처리시스템 접근권한 변경 또는 말소	○	○	○	
	③ 권한 부여 및 변경 말소 내역 최소 3년간 보관	○	○	○	
	④ 취급자별 한개의 접속계정사용, 공유금지	○	○	○	
	⑤ (취급자 or정보주체대상) PW 작성규칙수립 및 적용	○	○	○	
	⑥ ID or PW 일정횟수 오입력시 개인정보처리시스템 접근제한	○	○	X	
	⑦ 유형별 적용여부 규정임	–	–	–	
6조 개인정보 처리 시스템 접근통제	① 불법접근, 침해방지를 위해 다음 기능 포함조치 1. 접속권한을 IP주소, MAC주소 등으로 제한 2. 접속 IP등을 분석, 불법유출시도 탐지 및 대응	○	○	○	
	② 정보통신망으로 외부접속시 VPN or 전용선, 공인인증서 등 안전한 접속수단 적용	○	○	X	
	③ 인터넷홈페이지에서 (다른 법령에 근거하여) 성명, 주민번호로 본인확인시 추가인증수단제공	○	○	○	
	④ 홈페이지,P2P,공유설정,공개된 무선망으로 공개,유출되지 않도록 개인정보처리시스템, 컴퓨터, 모바일기기,관리용단말기 조치	○	○	○	[Network DLP] Mail-i [Endpoint DLP] Privacy-i
	⑤ 홈페이지에서 고유식별정보가 유출,변조,훼손되지 않도록 연1회 이상 취약점점검	○	○	X	[웹사이트 개인정보검출] 웹프라이버시
	⑥ 불법접근 및 침해사고방지를 위하여 취급자가 일정시간 이상 업무처리를 하지 않을 경우 자동으로 개인정보처리시스템접속 차단	○	○	X	
	⑦ 컴퓨터 or 모바일기기로 개인정보처리시 ① 미적용가능 OS나 보안프로그램 등에서 제공하는 접근통제기능을 사용한다	○	○	○	[모바일 내 검출,파기, 암호화솔루션]
	⑧ 모바일기기의 분실, 도난으로 개인정보가 유출, 변조, 훼손되지 않도록 모바일기기에 비밀번호설정을 해야 한다	○	○	○	
	⑨ 개인정보처리시스템 취약점점검 연1회이상, 보완조치 수행	○	X	X	접근통제솔루션 [DB] DB-i [WAS] WAS-i [SAP] App-i 서버 개인정보점검 Server-i
	⑩ 개인정보처리시스템 접속기록 점검결과 비인가자의 접속 등 개인정보처리시스템 취약점 발견시 즉시 보완조치	○	X	X	
	⑪ 유형별 적용여부 규정임	–	–	–	
7조 개인 정보의 암호화	① 고유식별정보, 비밀번호, 바이오정보를 정보통신망으로 송수신, 보조저장매체로 전달시 암호화	○	○	○	[DB]DB암호화 [서버]Server-i [PC, 매체] Privacy-i [DRM] [보안서버(SSL 외)]
	② 비밀번호,바이오정보는 암호화저장. 비밀번호는 복호화되지 않도록 일방향 암호화한다	○	○	○	
	③ 인터넷구간, 인터넷과 내부망의 중간지점(DMZ)에 고유식별정보 저장시 암호화	○	○	○	
	④ 내부망에 고유식별정보 저장시 암호화 적용여부 및 범위 1. 영향평가대상 공공기관 경우 영향평가결과에 따름 2. 위험도분석 결과에 따름	○	○	○	주민번호 경우 내부망에 있더라도 암호화 해야 함 100만명 미만 보관하는 처리자는 2016.12.31까지 100만명 이상 보관하는 처리자는 2017.12.31까지 적용
	⑤ (고유식별정보,비밀번호,바이오정보) 안전한 암호알고리즘으로 암호화저장	○	○	○	
	⑥ 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립 시행	○	X	X	
	⑦ 업무용 컴퓨터 또는 모바일기기에 고유식별정보저장시 상용암호화SW 또는 안전한 암호화 알고리즘으로 암호화저장	○	○	○	[PC] Privacy-i [모바일] Smart-i
	⑧ 유형별 적용여부규정	–	–	–	

조	내용	유형별 적용여부			보호조치
		유형3	유형2	유형1	
8조 접속기록의 보관 및 점검	① 개인정보처리시스템 접속기록 최소 6개월이상 보관/관리	○	○	○	접근통제솔루션 [D B] DB-i [WAS] WAS-i [SAP] App-i
	② 개인정보처리시스템 접속기록 반기별로 1회 이상 점검	○	○	○	
	③ 위·변조 및 도난, 분실되지 않도록 해당접속기록을 안전하게 보관	○	○	○	
9조 악성 프로그램 등 방지	~~키보드, 화면, 메모리탈취 등 신종/변종을 포함한~~ 악성프로그램등을 방지, 치료 할 수 있는 백신소프트웨어 등의 보안프로그램을 설치, 운영해야 하며 다음사항을 준수해야 한다 1. 보안프로그램 자동업데이트 사용 or 일 1회 이상 업데이트실시 2. 악성프로그램 경보발령 및 사용중인 응용프로그램이 OS·SW업체 보안업데이트 공지시 즉시 업데이트 실시 **3. 발견된 악성프로그램 등에 대해 삭제 등 대응조치**	○	○	○	[치료] 바이러스 백신 [방지] 세이프브라우징 솔루션 웹키퍼
유출사고 집단소송 판례 상의 고시9조 해석	**소만사의 의견: 9조에 2016년 유출사고 판결문 상의 해석을 반영해야 합니다** [기관 및 기업의 의무사항] ① 보안프로그램에는 특별한 사정이 없는 한 USB 쓰기 제한 기능이 있어야 하며 ② 그 기능이 작동하는지 관리·감독하는 조치가 수반되어야 함 [의무사항] 의 근거 · 일정규모이상 개인정보처리기관은 보안프로그램으로 PC에 USB를 연결하여 쓰기 기능을 사용하지 못하도록 제한하고 있는 점 · PC에 개인정보가 저장되어 있고 USB 쓰기 기능이 활성화된 경우 몰래 숨겨 반입/반출이 용이한 USB를 이용하여 쉽게 개인정보를 유출할 위험성이 매우 높아지는 점 · 크기가 작고 다른 물건으로 오인될 수 있도록 제작이 가능한 USB 자체의 반입/반출을 원천적으로 차단하는 데에는 한계가 있는 점 · PC에 있는 개인정보 등을 USB에 저장하여 유출할 가능성을 누구나 쉽게 예측할 수 있는 점				[USB쓰기제한 방지&관리감독] **DLP솔루션**
10조 관리용 단말기의 안전조치	**유출 등 침해사고방지를 위하여 관리용단말기에 다음의 안전조치** **1. 비인가자가 관리용단말기에 접근,임의조작 못하도록 조치** **2. 본래 목적외로 사용되지 않도록 조치** **3. 악성프로그램 감염방지등을 위한 보안조치 적용**	○	○	○	
11조 물리적 안전조치	① 전산실 자료보관실 등 물리적 보관장소에 대한 출입통제절차 수립/운영	○	○	○	Privacy-i 개인정보의 매체, 서류 복제를 최소화, 물리접근방지대상 최소화 효과
	② 개인정보포함 서류,보조저장매체 등을 잠금장치 있는 안전한장소에 보관	○	○	○	
	③ 개인정보포함 보조저장매체의 반출입통제를 위한 보안대책 마련 (별도의 개인정보처리시스템을 운영하지 않고 업무용컴퓨터 또는 모바일기기로 개인정보처리시 적용하지 않음)	○	○	○	
12조 재해/재난 대비 안전조치	**① 화재, 홍수, 단전 등 재해재난시 개인정보처리시스템보호를 위한 위기대응매뉴얼 등 대응절차를 마련하고 정기점검**	○	○	X	
	② 재해,재난발생시 개인정보처리시스템 백업 및 복구를 위한 계획마련	○	○	X	
	③ 유형별 적용여부 규정임	○	○	X	

조	내용	유형별 적용여부			보호조치
		유형3	유형2	유형1	
13조 파기	① 개인정보 파기시 다음 중 하나의 조치를 해야 한다 1. 완전파괴 (소각, 파쇄 등) 2. 전용소자장비를 이용하여 삭제 3. 데이터가 복원되지 않도록 초기화 or 덮어쓰기 수행	○	○	○	Privacy-i 복구 불가능 하도록 7회이상 파기
	② 개인정보의 일부만을 파기할 때에는 ①의 방법으로 파기하는 것이 어려운 경우 다음 각 호의 조치를 하여야 한다 1. 전자적파일 : 삭제 후 복구 및 재생되지 않도록 관리 및 감독 2. 제 1호 외의 기록물, 인쇄물, 서면 그 밖의 기록매체인 경우 해당 부분을 마스킹, 천공 등으로 삭제	○	○	○	
14조 수탁자에 대한 관리감독	**① 3자에게 개인정보처리업무 위탁시 수탁자는 해당 개인정보처리자의 안전조치 기준을 적용해야한다**	○	○	○	
	② 위탁시 처리자는 수탁자가 이 기준을 준수하는지 여부를 정기점검하고 수탁자는 이에 협조해야한다	○	○	○	
	③ 처리자는 ②점검에서 안전조치 기준위반등을 발견시 수탁자에게 적절한 안전조치 이행을 요청할 수 있다	○	○	○	

소만사의 의견: 9조에 2016년 유출사고 판결문 상의 해석을 반영해야 합니다



2) 개인정보 안전성 확보기준 제9조 위반 여부

가) 구 개인정보 보호법(2015. 7. 24. 법률 제13423호로 개정되기 전의 것, 이하 같다) 제29조, 같은 법 시행령 제30조 제1항 제5호를 구체화한 개인정보 안전성 확보조치 기준(행정안전부고시 제2011-43호, 이하 같다) 제9조에서는 개인정보처리자로 하여금 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 한다고 규정하고 있다. 한편, 피고를 포함한 각 [redacted] 보안프로그램을 통하여 업무용 컴퓨터에 USB 메모리를 연결하여 쓰기 기능을 사용하지 못하도록 제한하고 있는 점, 업무용 컴퓨터에 개인정보가 저장되어 있고 USB 메모리 쓰기 기능이 활성화된 경우 몰래 숨겨 반입·반출이 용이한 USB 메모리를 이용하여 쉽게 개인정보를 유출할 위험성이 매우 높아지는 점, 크기가 작고 다른 물건으로 오인될 수 있도록 제작이 가능한 USB 메모리 자체의 반입·반출을 원천적으로 차단하는 데에는 한계가 있는 점, 업무용 컴퓨터에 있는 개인정보 등을 USB 메모리에 저장하여 유출할 가능성을 누구나 쉽게 예측할 수 있는 점 등에 비추어 보면, 위 규정에 의하여 개인정보처리자가 설치·운영할 의무가 있는 보안프로그램에는 특별한 사정이 없는 한 USB 메모리의 쓰기 기능 사용을 제한하는 기능을 갖추고 있어야 하고, 그러한 기능이 실질적으로 작동하고 있는지 관리·감독하는 조치가 수반되어야 한다고 봄이 상당하다.

서울중앙지법 2016년 판결문

서울중앙지법 판결에 따르면 고시 9조의 〈보안프로그램〉의 기능은 다음을 포함한다

PC에서 USB로 개인정보 복제를 차단 + 개인정보 복제차단이 작동하는지 관리/감독

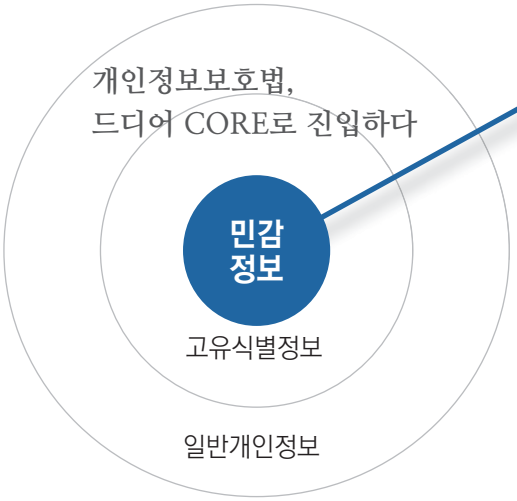
= **개인정보유출통제(DLP)**

발송일
2016. 04

3.22일 공포, 9.30일 시행 2016년 개정, 개인정보보호법 핵심변화 ①

〈민감정보〉에 개인정보보호법고시 〈개인정보의 안전성 확보조치 기준〉 미조치로 유출시 형사처벌, 몰수추징, 손해배상

개인정보보호법 원문보기 | 시행령 원문보기 | 이전 Report 보기



민감정보의 법적 정의
정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보

〈민감정보〉의 3대 딜레마	앞으로의 과제
1 가장 중요하지만 가장 식별하기 어렵다	산업별로 다양한 민감정보를 어떻게 정의하고 식별할 것인가?
2 가장 소량일 것 같지만 급속히 빅데이터화되고 있다	SNS, 동영상 등 비정형화된 빅데이터에서 민감정보를 어떻게 검색할 것인가?
3 유출되면 가장 피해가 크지만 법적처벌 없이 방치되어 있다	산업별로 다양한 민감정보를 어떻게 체계화하여 법제화할 것인가?

현재시점에서 〈민감정보〉의 3대 영역

1. 보건복지부 산하기관의 영역 (의료기관/약국/복지기관 외)

건강에 관한 정보 | **성생활**에 관한 정보 | **유전자**검사결과에 따른 유전자정보

2014 **보건복지부 가이드라인제정** (원칙적으로 법적구속력없음)
- 의료기관 가이드라인 (이전 Report 보기)
- 약국 가이드라인 (이전 Report 보기)
- 사회복지시설 가이드라인 (이전 Report 보기)

→ 2015 **대형사건 및 소송 발생** (법개정예고, 체크리스트 발표)

→ 2016 **개인정보보호법 개정**

〈안전성 확보조치 기준〉 미조치로 민감정보 유출시 **형사처벌, 몰수추징, 손해배상**

\+ **건강정보 보호법** 제정 추진

2. 법무부 산하기관의 영역 (경찰/검찰/보호관찰소 외)

〈형의 실효 등에 관한 법률〉 2조5호에 따른 다음의 **범죄경력자료**

가. 벌금 이상의 형의 선고, 면제 및 선고유예 나. 보호감호, 치료감호, 보호관찰
다. 선고유예의 실효 라. 집행유예의 취소
마. 벌금 이상의 형과 함께 부과된 몰수, 추징, 사회봉사명령, 수강명령 등의 선고 또는 처분

*수강명령은 유죄가 인정된 의존/중독성 범죄자를 일정시간 보호관찰소 또는 지정 전문기관에서 교육을 받도록 명하는 제도이다. 교육내용으로는 약물오남용 방지교육, 준법운전, 알코올남용 방지교육, 정신/심리치료교육, 성폭력 방지교육 등이 있다.

3. 정당/단체/SNS/게시판의 영역

- 사상 및 신념
- 노동조합/정당의 가입 및 탈퇴
- 정치적 견해

민감정보에 〈개인정보보호법고시〉 미적용시 처벌

2016.9.30부터 고발 및 대표자 징계 규정 대상

시행중

법규위반에 따른 범죄혐의시
관할수사기관에
1. 행자부가 개인정보처리자 고발 가능
2. 중앙행정기관은 산하기관 고발 가능

65조 ①항, ③항

+

시행중

법규위반시 징계자로
대표자(기관장, CEO) 명시
중앙행정기관은 산하기관
기관장 징계가능

65조 ②항, 3항 65조 ①항

2016.9.30부터

과태료
3천만원 이하

74조의2

민감정보에 〈개인정보보호법고시〉 미적용으로 유출시 처벌

2016.9.30부터

형사처벌
2년 이하 징역 or
2천만원 이하 벌금

73조

2016.9.30부터 몰수 추징 대상

시행중

안전성 확보에 필요한 조치를
하지 아니하여
개인정보를 분실/도난/유출/
위조/변조 or 훼손당한 자

+

몰수, 추징
해당 위반행위와 관련하여 취득한 금품이나
그 밖의 이익은 몰수할 수 있으며,
불가능할 경우 그 가액을 추징할 수 있다. 74조의2

* 가액(價額): 물건의 가치에 상당한 금액

+

2016.7.25부터 시행

실제 손해가 발생한 때

〈징벌적 손해배상〉 피해액의 3배까지 배상

개인정보보호법 39조 ③항
고의 or 중대한 과실로 개인정보가 분실/도난/유출/위조/변조
or 훼손되어 정보주체에게 손해가 발생한 때 법원은
그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다
* 예외: 고의 or 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다

〈법정 손해배상〉 300만원까지 배상

개인정보보호법 39조의 2
① 고의 or 과실로 개인정보가 분실/도난/유출/위조/변조 or 훼손된 때 300만원 이하 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다.
② 법원은 변론전체의 취지와 증거조사의 결과를 고려하여 300만원 이하 범위에서 손해액을 인정할 수 있다. * 예외: 고의 or 중대한 과실이 없음을 증명한 경우
③ 제39조에 따라 손해배상을 청구한 정보주체는 사실심(事實審)의 변론이 종결되기 전까지 그 청구를 ①항에 따른 청구로 변경할 수 있다.

손해배상 청구 절차

개인정보 유출 사고 발생

정보주체

피해입증이 가능시 〈징벌적 손해배상〉 청구

피해입증 불가능시 〈법정 손해배상〉 청구

개인정보처리자

고의 · 과실이 없었음을 입증

고시를 100% 준수했음을 입증해야 함

입증 못하면 배상

법원

〈피해액의 3배내〉에서 배상액산정

〈300만원 내〉에서 배상액 산정

법원의 배상액 산정시 고려사항	
위반행위로 인한 혹은 위반행위의	피해 규모
	〈서비스 제공자〉가 취득한 경제적 이익
	벌금 및 과징금
	기간 · 횟수 등
〈서비스 제공자〉의	재산상태
	고의 or 손해발생의 우려를 인식한 정도
〈서비스 제공자〉가	개인정보 분실 · 도난 · 유출 후 해당 개인정보 회수를 위해 노력한 정도
	이용자의 피해구제에 노력한 정도

〈개인정보의 안전성 확보조치 기준〉 상세규정 보기 1/2

<table>
<tr><th>조항</th><th>개정여부</th><th>내용</th></tr>
<tr><td rowspan="2">23조
(민감정보
처리제한)</td><td>기존</td><td>① 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보,
그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서
대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리해서는 안된다.
1. 별도로 동의를 받은 경우
2. 법령에서 민감정보처리를 요구하거나 허용하는 경우 가능
→ 위반시 5년 이하 징역 5천만원 이하 벌금</td></tr>
<tr><td>신설</td><td>② 민감정보 처리시 민감정보가 분실/도난/유출/위조/변조 or 훼손되지 아니하도록
29조에 따른 〈안전성 확보에 필요한 조치〉를 하여야 한다.
→ 미조치시 과태료 3천만원 이하 (75조 ②항 6호),
미조치로 유출시 2년 이하 징역 2천만원 벌금 (73조)</td></tr>
<tr><td>29조
(안전조치
의무)</td><td>개정</td><td>내부관리계획 수립, 접속기록 보관 등 대통령령에 따라
안전성 확보에 필요한 기술적/관리적/물리적 조치를 하여야 한다.</td></tr>
<tr><td rowspan="2">39조
(손해배상
책임)</td><td>기존</td><td>① 정보주체는 개인정보처리자의 법 위반행위로 손해를 입으면 손해배상을 청구할 수 있다.
개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.</td></tr>
<tr><td>신설</td><td>② 고의 or 중대과실로 개인정보가
분실/도난/유출/위조/
변조/훼손되어
정보주체에게 손해가 발생한 때
법원은 손해액의 3배를
넘지 아니하는 범위에서
배상액을 정할 수 있다.

<table><tr><th colspan="2">법원의 배상액 산정시 고려사항</th></tr><tr><td rowspan="2">위반행위로 인한 or
위반행위의</td><td>피해 규모, 〈서비스 제공자〉가 취득한 경제적 이익</td></tr><tr><td>벌금 및 과징금, 기간 · 횟수 등</td></tr><tr><td>〈서비스 제공자〉의</td><td>재산상태, 고의 or 손해발생의 우려를 인식한 정도</td></tr><tr><td rowspan="2">〈서비스 제공자〉가</td><td>개인정보 분실 · 도난 · 유출 후 회수를 위해 노력한 정도</td></tr><tr><td>이용자의 피해구제에 노력한 정도</td></tr></table></td></tr>
<tr><td>39조2
(법정
손해배상
청구)</td><td>신설</td><td>① 고의 or 과실로 개인정보가 분실/도난/유출/위조/변조/훼손시
300만원 이하 손해액으로 배상을 청구할 수 있다. *예외: 고의 or 중대과실 없음 증명시
② 법원은 ①에 따른 청구시 변론전체의 취지와 증거조사결과를 고려, 손해액을 인정할 수 있다.
③ 징벌적 손해배상을 청구한 정보주체는 사실심변론 종결전까지 법정손해배상으로
변경청구가능</td></tr>
</table>

〈개인정보의 안전성 확보조치 기준〉 상세규정 보기 2/2

<table>
<tr><th>조항</th><th>개정여부</th><th>내용</th></tr>
<tr><td>74조의2
(몰수/
추징 등)</td><td>신설</td><td>
<table>
<tr><th>조</th><th>내용</th><th>처벌</th></tr>
<tr><td>70조</td><td colspan="2">① 공공기관에서 처리중인 개인정보를 변경,말소 → 심각한 지장을 초래한 자</td><td rowspan="2">10년 징역
or
1억 벌금</td></tr>
<tr><td>② 거짓, 부정으로 개인정보를 취득 후 영리,부정한 목적으로 제3자에게 제공한 자, 교사/알선자</td></tr>
<tr><td rowspan="4">71조</td><td rowspan="3">정보주체의 동의를 받지 아니하고</td><td>①, ② 개인정보를 3자에게 제공한 자 및 그 사정을 알고 제공받은 자</td><td rowspan="4">5년 징역
or
5천 벌금</td></tr>
<tr><td>③ 〈민감정보〉를 처리한 자</td></tr>
<tr><td>④ 고유식별정보를 처리한 자</td></tr>
<tr><td colspan="2">⑤ 업무상 개인정보를 누설, 제공한 자 및 영리,부정한 목적으로 제공받은 자</td></tr>
<tr><td rowspan="3">72조</td><td colspan="2">⑥ (권한없이) 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출한 자</td></tr>
<tr><td colspan="2">① 영상정보처리기기의 설치목적과 다른 목적으로 임의조작, 다른 곳을 비추는 자 , 녹음한 자</td><td rowspan="3">3년징역
or
3천 벌금</td></tr>
<tr><td colspan="2">② 거짓, 부정으로 개인정보를 취득, 동의받은 자 및 사정을 알면서 영리,부정한 목적으로 제공받은 자</td></tr>
<tr><td colspan="2">③ 개인정보보호위원회, 영향평가, 분쟁조정위원회 업무상 알게 된 비밀을 누설, 직무 외로 이용한 자</td></tr>
<tr><td rowspan="3">73조</td><td>①. 〈민감정보〉에 신규적용</td><td>24조③ (고유식별정보) ,
25조⑥ (영상정보처리기기)
29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실/도난/유출/위조/변조 or 훼손당한 자</td><td rowspan="3">2년 징역
or
2천 벌금</td></tr>
<tr><td colspan="2">② 정보주체의 요구시에도 정정/삭제 등 조치를 하지 아니하고 개인정보를 계속 이용, 제3자에게 제공한 자</td></tr>
<tr><td colspan="2">③ 정보주체의 요구시에도 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 자</td></tr>
</table>
몰수, 추징
해당 위반행위와 관련하여 취득한 금품이나 그 밖의 이익은 몰수할 수 있으며, 불가능할 경우 그 가액을 추징할 수 있다
</td></tr>
<tr><td>65조
(고발 및
징계권고)</td><td>기존</td><td>
<table>
<tr><th>조항</th><th>누가</th><th>누구에게</th><th colspan="2">어떤 경우</th><th>어떤 처벌을 하는가</th></tr>
<tr><td>65조①</td><td rowspan="2">행정
자치부</td><td rowspan="2">개인정보
처리자</td><td rowspan="4">개인정보
보호법규
위반으로</td><td>위반행위에 따른 범죄혐의 인정시</td><td>관할 수사기관에 고발</td></tr>
<tr><td>65조②</td><td>위반행위가 있다고 인정시</td><td>책임자(대표자, 임원)징계를 권고
개인정보처리자는 그 결과를 행자부에 통보</td></tr>
<tr><td rowspan="2">65조③</td><td rowspan="2">중앙
행정기관</td><td rowspan="2">소속
기관, 단체</td><td>위반행위에 따른 범죄혐의 인정시</td><td>관할 수사기관에 고발</td></tr>
<tr><td>위반행위가 있다고 인정시</td><td>책임자(대표자, 임원)징계를 권고
소속기관, 단체는 그 결과를
중앙행정기관에 통보</td></tr>
</table>
</td></tr>
</table>

발송일
2016. 04

3.22일 공포, 9.30 시행 2016년 개정, 개인정보보호법 핵심변화 ②

〈고유식별정보〉에 개인정보보호법고시 〈개인정보의 안전성 확보조치 기준〉 미조치로 유출시 형사처벌, 몰수추징, 손해배상

개인정보보호법 원문보기 | 시행령 원문보기 | 이전 Report 보기

운전면허번호 | 여권번호 | 외국인등록번호

그리고 주민등록번호

1. 주민등록번호에 〈개인정보의 안전성 확보조치 기준〉상의 〈안전성 확보조치〉 강화

~2016.08.07까지	~2017.01.01까지	~2018.01.01까지
점검 → 파기	(저장된 주민번호 명수가) 100만명 미만일 경우 내부망 주민등록번호 암호화완료	(저장된 주민번호 명수가) 100만명 이상일 경우 내부망 주민등록번호 암호화완료
법령 근거없는 주민등록번호 파기완료	점검 → 암호화	

이전 Report 보기 | 이전 Report 보기 | 이전 Report 보기

2. 주민등록번호를 수집할 수 있는 법령내역 구체화(2017.03.30까지) → 개인정보 보호위원회에서 매년 정기국회시 법령현황 제출

3. 고유식별정보에 행자부 정기감사 → 행자부권한 처벌

2016.09.30 부터~

일정기준이상 기관/기업대상으로 고유식별정보(특히 주민등록번호)에 〈안전성 확보조치 기준〉 적용여부를 행자부가 정기적으로 조사

행자부권한으로 가능한 처벌
- 수사기관에 고발
- 대표자(기관장, CEO)징계
- 과태료 , 과징금

4. 유출시 손해배상

2016.07.25 부터~

손해배상

고유식별정보(특히 주민등록번호)에 〈안전성 확보조치 기준〉 미적용으로 유출시 법정손해배상 or 징벌적손해배상

고유식별정보에 〈개인정보보호법고시〉 미적용시 처벌

시행중

법규위반에 따른 범죄혐의시 관할수사기관에
1. 행자부가 개인정보처리자 고발 가능
2. 중앙행정기관은 산하기관 고발 가능

65조 ①항, ③항

시행중

법규위반시 징계자로
대표자(기관장, CEO) 명시

중앙행정기관은 산하기관 기관장 징계가능

65조 ②항, ③항 65조 ①항

시행중

과태료
3천만원 이하

74조의2

고유식별정보에 〈개인정보보호법고시〉 미적용으로 유출시 처벌

시행중

과징금

위반행위 관련
매출의 3%까지 징수

73조

시행중

주민등록번호 유출시 과징금

5억까지 징수

34조의 2

시행중

형사처벌

2년 이하 징역 or 2천만원 이하 벌금

73조

+

시행중

몰수, 추징

해당 위반행위와 관련하여 취득한 금품이나 그 밖의 이익은 몰수할 수 있으며,
불가능할 경우 그 가액을 추징할 수 있다. 74조의2

* 가액(價額): 물건의 가치에 상당한 금액

+

2016.7.25부터 시행

실제 손해가 발생한 때

〈징벌적 손해배상〉 피해액의 3배까지 배상

개인정보보호법 39조 ③
고의 or 중대한 과실로 개인정보가 분실/도난/유출/위조/변조 or 훼손되어 정보주체에게 손해가 발생한 때 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다
* 예외: 고의 or 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다

〈법정 손해배상〉 300만원까지 배상

개인정보보호법 39조의2
① 고의 or 과실로 개인정보가 분실/도난/유출/위조/변조 or 훼손된 때 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다.
② 법원은 변론전체의 취지와 증거조사의 결과를 고려하여 300만원 이하범위에서 손해액을 인정할 수 있다. * 예외: 고의 or 중대한 과실이 없음을 증명한 경우
③ 39조에 따라 손해배상을 청구한 정보주체는 사실심(事實審)의 변론이 종결되기 전까지 그 청구를 ①항에 따른 청구로 변경할 수 있다.

손해배상 청구 절차

개인정보 유출 사고 발생

정보주체

- 피해입증이 가능시 〈징벌적 손해배상〉 청구
- 피해입증 불가능시 〈법정 손해배상〉 청구

개인정보처리자

고의 · 과실이 없었음을 입증

고시를 100% 준수했음을 입증해야 함

입증 못하면 배상

법원

- 〈피해액의 3배내〉에서 배상액산정
- 〈300만원 내〉에서 배상액 산정

법원의 배상액 산정시 고려사항	
위반행위로 인한 혹은 위반행위의	피해 규모
	〈서비스 제공자〉가 취득한 경제적 이익
	벌금 및 과징금
	기간 · 횟수 등
〈서비스 제공자〉의	재산상태
	고의 or 손해발생의 우려를 인식한 정도
〈서비스 제공자〉가	개인정보 분실 · 도난 · 유출 후 해당 개인정보 회수를 위해 노력한 정도
	이용자의 피해구제에 노력한 정도

〈개인정보의 안전성 확보조치 기준〉 상세규정 보기 1/2

<table>
<tr><th>조항</th><th>개정여부</th><th>내용</th></tr>
<tr><td rowspan="3">24조
(고유
식별정보의
처리제한)</td><td>2015
개정</td><td>③ 〈고유식별정보〉 처리시 분실/도난/유출/위조/변조/훼손되지 않도록
대통령령에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다</td></tr>
<tr><td rowspan="2">신설</td><td>④ 행자부장관은 처리하는 개인정보의 종류/규모, 종업원수, 매출액에 따라 대통령령으로 정하는
개인정보처리자가 ③에 따라 안전성 확보에 필요한 조치를 하였는지 정기적으로 조사해야 한다</td></tr>
<tr><td>⑤ 행자부장관은 대통령령으로 정하는 전문기관으로 하여금
④에 따른 조사를 수행하게 할 수 있다</td></tr>
<tr><td>29조
(안전조치
의무)</td><td>기존</td><td>내부 관리계획 수립, 접속기록 보관 등 대통령령에 따라
안전성 확보에 필요한 기술적/관리적 및 물리적 조치를 하여야 한다</td></tr>
<tr><td rowspan="3">24조의2
(주민
등록번호
처리제한)</td><td>신설</td><td>① 다음 경우를 제외하고는 주민등록번호를 처리할 수 없다
1. 법률/대통령령/국회규칙/대법원규칙/헌법재판소규칙/중앙선거관리위원회규칙 및 감사원규칙에서
구체적으로 처리를 요구, 허용한 경우 (시행일 2017.03.30)</td></tr>
<tr><td rowspan="2">기존</td><td>② 주민등록번호가 분실/도난/유출/위조/변조 또는 훼손되지 아니하도록 암호화 조치를 통하여
안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은
개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.</td></tr>
<tr><td>③ 개인정보처리자는 ① 각 호에 따라 주민등록번호를 처리하는 경우에도
정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는
주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다</td></tr>
<tr><td rowspan="2">34조의2
(과징금의
부과 등)</td><td rowspan="2">2015
개정</td><td>① 주민등록번호가 분실/도난/유출/위조/변조 또는 훼손된 경우, 5억원 이하의 과징금을 부과/징수한다
*예외: 24조 ③에 따른 안전성 확보에 필요한 조치를 다한 경우</td></tr>
<tr><td>② 행정자치부장관은 ①에 따른 과징금 부과시 다음 사항을 고려하여야 한다.
1. 24조 ③에 따른 안전성 확보에 필요한 조치 이행 노력정도
2. 분실 · 도난 · 유출 · 위조 · 변조 · 훼손된 주민등록번호의 정도
3. 피해확산 방지를 위한 후속조치 이행 여부</td></tr>
<tr><td rowspan="2">39조
(손해배상
책임)</td><td>기존</td><td>① 정보주체는 개인정보처리자의 법 위반행위로 손해를 입으면 손해배상을 청구할 수 있다.
개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.</td></tr>
<tr><td>신설</td><td>② 고의 or 중대과실로
개인정보가 분실/도난/유출/
위조/변조/훼손되어
정보주체에게 손해가 발생한 때
법원은 손해액의 3배를
넘지 아니하는 범위에서
배상액을 정할 수 있다.

<table>
<tr><th colspan="2">법원의 배상액 산정시 고려사항</th></tr>
<tr><td rowspan="2">위반행위로 인한
혹은 위반행위의</td><td>피해 규모, 〈서비스 제공자〉가 취득한
경제적 이익</td></tr>
<tr><td>벌금 및 과징금, 기간 · 횟수 등</td></tr>
<tr><td>〈서비스 제공자〉의</td><td>재산상태, 고의 or 손해발생의
우려를 인식한 정도</td></tr>
<tr><td rowspan="2">〈서비스 제공자〉가</td><td>개인정보 분실 · 도난 · 유출 후
회수를 위해 노력한 정도</td></tr>
<tr><td>이용자의 피해구제에 노력한 정도</td></tr>
</table>
</td></tr>
<tr><td>39조2
(법정
손해배상
청구)</td><td>신설</td><td>① 고의 or 과실로 개인정보가 분실/도난/유출/위조/변조/훼손시
300만원 이하 손해액으로 배상을 청구할 수 있다.
*예외: 고의 or 중대과실 없음 증명시</td></tr>
</table>

〈개인정보의 안전성 확보조치 기준〉 상세규정 보기 1/2

<table>
<tr><th>조항</th><th>개정여부</th><th>내용</th></tr>
<tr><td>67조
(연차보고)</td><td>신설</td><td>① 〈개인정보보호위원회〉는 관계기관 등으로부터 자료를 제출받아 매년
〈개인정보 보호시책의 수립 및 시행에 관한 보고서〉를 작성, 정기국회 개회 전까지 국회에 제출해야 한다
② 보고서내용은 아래와 같다.
1. 정보주체의 권리침해 및 구제현황 2. 개인정보처리실태조사 결과
3. 개인정보 보호시책의 추진현황 및 실적 4. 해외입법 및 정책 동향
5. 주민등록번호 처리관련 법률/대통령령/국회규칙/대법원규칙/헌법재판소규칙/
중앙선거관리위원회규칙 및 감사원규칙의 제/개정 현황
6. 기타 (시행일 2017.03.30)</td></tr>
<tr><td>74조의2
(몰수/추징
등)</td><td>신설</td><td>
<table>
<tr><th>조</th><th>내용</th><th>처벌</th></tr>
<tr><td>70조</td><td colspan="2">① 공공기관에서 처리중인 개인정보를 변경,말소→ 심각한 지장을 초래한 자</td><td rowspan="2">10년 징역
or
1억 벌금</td></tr>
<tr><td colspan="2">② 거짓, 부정으로 개인정보를 취득 후 영리,부정한 목적으로 제3자에게 제공한 자, 교사 · 알선자</td></tr>
<tr><td rowspan="4">71조</td><td rowspan="3">정보주체의 동의를 받지 아니하고</td><td>①, ② 개인정보를 3자에게 제공한 자 및 그 사정을 알고 제공받은 자</td><td rowspan="4">5년 징역
or
5천 벌금</td></tr>
<tr><td>③ 〈민감정보〉를 처리한 자</td></tr>
<tr><td>④ 고유식별정보를 처리한 자</td></tr>
<tr><td colspan="2">⑤ 업무상 개인정보를 누설, 제공한 자 및 영리,부정한 목적으로 제공받은 자</td></tr>
<tr><td rowspan="3">72조</td><td colspan="2">⑥ (권한없이) 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출한 자</td></tr>
<tr><td colspan="2">① 영상정보처리기기의 설치목적과 다른 목적으로 임의조작, 다른 곳을 비추는 자 , 녹음한 자</td><td rowspan="3">3년징역
or
3천 벌금</td></tr>
<tr><td colspan="2">② 거짓, 부정으로 개인정보를 취득, 동의받은자 및 사정을 알면서 영리,부정한 목적으로 제공받은 자</td></tr>
<tr><td colspan="2">③ 개인정보보호위원회, 영향평가, 분쟁조정위원회 업무상 알게 된 비밀을 누설, 직무 외로 이용한 자</td></tr>
<tr><td rowspan="3">73조</td><td colspan="2">① 24조 ③ (고유식별정보) , 25조 ⑥ (영상정보처리기기), 29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실/도난/유출/위조/변조 or 훼손당한 자</td><td rowspan="3">2년 징역
or
2천 벌금</td></tr>
<tr><td colspan="2">② 정보주체의 요구시에도 정정/삭제 등 조치를 하지 아니하고 개인정보를 계속 이용, 제3자에게 제공한 자</td></tr>
<tr><td colspan="2">③ 정보주체의 요구시에도 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 자</td></tr>
</table>
+ 몰수, 추징
해당 위반행위와 관련하여 취득한 금품이나 그 밖의 이익은 몰수할 수 있으며, 불가능할 경우 그 가액을 추징할 수 있다.
</td></tr>
<tr><td>65조
(고발 및
징계권고)</td><td>기존</td><td>
<table>
<tr><th>조항</th><th>누가</th><th>누구에게</th><th colspan="2">어떤 경우</th><th>어떤 처벌을 하는가</th></tr>
<tr><td>65조①</td><td rowspan="2">행정
자치부</td><td rowspan="2">개인정보
처리자</td><td rowspan="4">개인정보
보호법규
위반으로</td><td>위반행위에 따른 범죄혐의 인정시</td><td>관할 수사기관에 고발</td></tr>
<tr><td>65조②</td><td>위반행위가 있다고 인정시</td><td>책임자(대표자, 임원)징계를 권고
개인정보처리자는 결과를 행자부에 통보</td></tr>
<tr><td rowspan="2">65조③</td><td rowspan="2">중앙
행정기관</td><td rowspan="2">소속
기관, 단체</td><td>범죄혐의 인정시</td><td>관할 수사기관에 고발</td></tr>
<tr><td>위반행위가 있다고 인정시</td><td>책임자(대표자, 임원)징계를 권고
소속기관, 단체는 결과를
중앙행정기관에 통보</td></tr>
</table>
</td></tr>
</table>

발송일
2015. 09

2015년 하반기 공포예정 개인정보보호법 대통령령 개정안에 따른

내부망에 보관한 주민등록번호 암호화 완료일입니다

주민등록번호 999,999명까지
2017년 1월1일

100만명 기준으로

주민등록번호 100만명부터
2018년 1월 1일

지금 무엇을 해야할까요?

DB서버, 웹서버, PC, 모바일까지
모두 진단하여서 보관되어있는 주민등록번호가 100만명 미만인지 이상인지 확인해야 합니다

법에서 내부망 주민등록번호까지 암호화해야 함을 규정

2014년 3월
개인정보보호법 개정

개인정보보호법 24조의2
② 주민등록번호가
분실/도난/유출/변조
or 훼손되지 아니하도록
암호화조치를 통하여
안전하게 보관하여야 한다.
이 경우 암호화적용대상/
대상별적용시기등에 관하여
필요한 사항은
개인정보의 처리규모와
유출시 영향 등을 고려하여
대통령령으로 정한다.

대통령령에서 암호화 완료시기 규정

2015년 7월
개인정보보호법 대통령령 개정

개인정보보호법
대통령령 21조의2
② 암호화적용시기는 다음 각 호와 같다
1. 100만명 미만
주민등록번호보관
2017년 1월 1일
2. 100만명 이상
주민등록번호 보관
2018년 1월 1일

③ 행정자치부장관은
기술적,경제적 타당성을 고려하여
암호화조치의 세부적사항을
정하여 고시할 수 있다.

향후 고시에서 암호화조치 세부내용 규정 예정

발송일
2016. 05

이 개인정보처리자는 누구일까요? 레터 ①

귀사가 이 경우에 해당한다면 〈고유식별정보〉에 〈개인정보의 안전성 확보조치 기준〉 조치여부를 행자부에 2년에 1번씩 감사받게 됩니다

개인정보보호법 원문보기 시행령 원문보기 이전 Report 보기

공공기관 or 5만명 이상 고유식별정보 처리자 대상으로

· 누가	행정자치부, KISA
· 언제부터	2016.9.30일부터 시행
· 어떤 주기로	2년에 한번씩
· 무엇을	고유식별정보에
· 어떻게 감사하는가?	〈개인정보의 안전성 확보조치 기준〉 적용여부를 온라인 or 서면 자료제출 방식으로 감사

다음 경우는 행정자치부 공무원이 직접 방문하여 감사

1. 행정자치부 장관이 요청한 자료를 제출하지 아니한 경우

2. 다음 규정의 위반사항 or 협의발견시 **3.다음 규정의 위반신고 or 민원 접수시**

고유식별 정보규정 법24조	① 고유식별정보처리를 위해서는 1. (다른 개인정보와) 별도로 동의받아야 함 2. 법령에서 허용해야 함
	③ 〈고유식별정보〉에 암호화 등 안전성 확보에 필요한 조치를 해야 함
(고유식별정보 중) 주민등록 번호규정 법24조의2	① 주민등록번호를 처리할 수 있는 경우 (시행일 2017.03.30) 1. 법률/대통령령/국회규칙/대법원규칙/헌법재판소규칙/중앙선관위 규칙 및 감사원규칙에서 구체적으로 처리를 요구, 허용한 경우
	② 주민등록번호 암호화 (주민번호 100만명 미만 보관시 2017.1월.1일까지,100만명 이상 보관시 2018. 1월. 1일까지 완료)
	③ 홈페이지 회원가입단계에서 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공

어떤 처벌이 가능한가?

행자부권한으로 가능한 처벌

· 수사기관에 고발 · 대표자(기관장, CEO)징계 · 과태료/과징금 부과

지금 무엇을 해야할까요?

DB서버, 웹서버, PC, 모바일, USB, 출력물까지 모두 점검하여서

고유식별정보 특히 주민등록번호가 얼마나 있는지 확인해야 합니다

〈고유식별정보 처리〉관련 상세규정 보기

<table>
<tr><th>조항</th><th>개정여부</th><th>내용</th></tr>
<tr><td rowspan="3">법 24조
(고유 식별정보의 처리제한)</td><td>2015 개정</td><td>③ 〈고유식별정보〉 처리시 분실/도난/유출/위조/변조/훼손되지 않도록
대통령령에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다</td></tr>
<tr><td>2016 신설</td><td>④ 행자부장관은 처리하는 개인정보의 종류/규모, 종업원수, 매출액에 따라 대통령령으로 정하는
개인정보처리자가 ③에 따라 안전성 확보에 필요한 조치를 하였는지 정기적으로 조사해야 한다</td></tr>
<tr><td>⑤ 행자부장관은 대통령령으로 정하는 전문기관으로 하여금 ④에 따른 조사를 수행하게 할 수 있다</td></tr>
<tr><td rowspan="2">법 24조의2
(주민 등록번호 처리제한)</td><td>2016 신설</td><td>① 다음 경우를 제외하고는 주민등록번호를 처리할 수 없다
1. 법률/대통령령/국회규칙/대법원규칙/헌법재판소규칙/중앙선거관리위원회규칙 및
감사원규칙에서 구체적으로 처리를 요구, 허용한 경우 (시행일 2017.03.30)</td></tr>
<tr><td>2015 개정</td><td>② 주민등록번호가 분실/도난/유출/위조/변조 또는 훼손되지 아니하도록 암호화 조치를 통하여
안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여
필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.
③ 개인정보처리자는 ①항 각 호에 따라 주민등록번호를 처리하는 경우에도
정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는
주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다</td></tr>
<tr><td>시행령 18조
(고유 식별정보의 처리제한)</td><td>2016 신설</td><td>② 법 24조 ④에 따른 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 다음 각 호와 같다.
1. (법 2조 6호에 따른) 공공기관
* 법 2조 6호: "공공기관"이란 다음 각 목의 기관을 말한다.
가. 국회, 법원, 헌법재판소, 중앙선관위 행정사무 처리기관, 중앙행정기관(대통령/국무총리 소속기관 포함), 그 소속기관, 지방자치단체
나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관
2. 5만명 이상의 정보주체에 관하여 (법 24조에 따른) 고유식별정보를 처리하는 자
③ 행정자치부장관은 ②의 개인정보처리자를 대상으로 고유식별정보의
안전성 확보조치 여부를 매 2년마다 1회 이상 조사하여야 한다.
④ 법 24조 ④항에 따른 조사는 ②항 각 호에 해당하는 개인정보처리자에게
온라인 또는 서면을 통하여 필요한 자료를 제출하게 하는 방법으로 수행한다.
⑤ 행자부장관은 대통령령으로 정하는 전문기관으로 하여금 ④에 따른 조사를 수행하게 할 수 있다
<table>
<tr><th>호</th><th colspan="3">내용</th></tr>
<tr><td>1</td><td colspan="3">1. 행정자치부장관이 요청한 자료를 제출하지 아니한 경우</td></tr>
<tr><td rowspan="3">2</td><td rowspan="3">2. 다음규정의 위반사항 or 혐의발견
3. 위반신고 or 민원접수시</td><td rowspan="2">법 24조</td><td>① 고유식별정보처리를 위해서는
1. (다른 개인정보와) 별도로 동의받아야함 2. 법령에서 허용해야 함</td></tr>
<tr><td>③ 〈고유식별정보〉에 암호화 등 안전성확보에 필요한 조치를 해야함</td></tr>
<tr><td>법 24조의 2</td><td>① 주민등록번호를 처리할 수 있는 경우 (시행일 2017.03.30)
1. 법률/대통령령/국회규칙/대법원규칙/헌법재판소규칙/
중앙선거관리위원회규칙 및 감사원규칙에서
구체적으로 처리를 요구, 허용한 경우
② 주민등록번호를 암호화하지 않은 경우, 2017년 2018년
③ 주민등록번호 처리시 홈페이지 회원가입단계에서 주민등록번호를
사용하지 아니하고도 회원으로 가입할 수 있는 방법 제공</td></tr>
</table>
⑥ 법 24조 ⑤에서 "대통령령으로 정하는 전문기관"이란
〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉 52조에 따른 한국인터넷진흥원을 말한다.</td></tr>
</table>

발송일
2016. 05

이 개인정보처리자는 누구일까요? 레터 ②

귀사가 이 경우에 해당한다면 개인정보를 제공받은 경우 3개월이내에, 정보주체에게 1:1로, 제공받았다는 사실을 알려줘야 합니다

개인정보보호법 원문보기 | 시행령 원문보기 | 이전 Report 보기

5만명 이상 민감정보 or 고유식별정보 처리자
or
100만명 이상 개인정보처리자

· 언제부터	2016.9.30일부터 시행
· 어떤 경우	(다른 처리자로부터) 연락처를 포함한 **개인정보를 제공받은 때**
· 누구에게	제공받은 개인정보의 **정보주체에게**
· 무엇을	개인정보의 1.수집출처(제공받은 출처) 2.처리목적 3. 처리정지를 요구할 권리가 있다는 사실을
· 어떤 기한 내에	제공받은날로부터 **3개월** 이내에
· 어떤 방법으로	**서면·전화·문자전송·전자우편 등**의 방법으로 알림 *알린 사실을(시기, 방법 포함) 해당정보 파기시까지 관리해야 함

[예외] 공공기관 개인정보파일등록 및 공개대상에서 제외되는 파일은 예외

1. 국가 안전, 외교상 비밀, 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄수사, 공소제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일
3. 조세범처벌법에 따른 범칙행위 조사 및 관세법에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
4. 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일
5. 다른 법령에 따라 비밀로 분류된 개인정보파일

9.30일부터 무엇을 해야할까요?

DB서버, 웹서버, PC, 모바일, USB, 개인정보출력까지
주기적으로 점검하여서
제공받은 개인정보가 있는지 확인해야 합니다

〈개인정보 수집사실 고지〉관련 상세규정 보기

조항	개정여부	내용
법 17조 (개인정보의 제공)	기존	① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다.)할 수 있다. 1. 정보주체의 동의를 받은 경우
법 20조 (정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지)	기존	① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 다음 각 호의 모든 사항을 정보주체에게 알려야 한다. 1. 개인정보의 수집 출처 2. 개인정보의 처리 목적 3. 37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실
	2016 신설	② 처리하는 개인정보의 종류 · 규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제17조 ①항 1호에 따라 정보주체 이외로부터 개인정보를 수집하여 처리하는 때에는 ①항 각 호의 모든 사항을 정보주체에게 알려야 한다. 다만, 개인정보처리자가 수집한 정보에 연락처 등 정보주체에게 알릴 수 있는 개인정보가 포함되지 아니한 경우에는 그러하지 아니하다.
		③ ②항 본문에 따라 알리는 경우 정보주체에게 알리는 시기/방법 및 절차 등 필요한 사항은 대통령령으로 정한다.
	2016 부분개정	④ ①항과 ②항 본문은 다음 각 호의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다. 1. 고지요구대상이 되는 개인정보가 제32조 ②항 각 호의 하나에 해당하는 개인정보파일에 포함되어 있는 경우 2. 고지로 인하여 다른 사람의 생명/신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
법 32조 (개인정보파일의 등록 및 공개)	기존	② 다음 각 호의 어느 하나에 해당하는 개인정보파일에 대하여는 ①항(개인정보파일 등록 및 공개)을 적용하지 아니한다. 1. 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일 2. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일 3. 조세범처벌법에 따른 범칙행위 조사 및 관세법에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일 4. 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일 5. 다른 법령에 따라 비밀로 분류된 개인정보파일
대통령령 (=시행령) **15조의2** (개인정보 수집 출처 고지 대상/방법/절차 등)	2016 신설	① 법 20조 ②항의 〈대통령령으로 정하는 기준에 해당하는 개인정보처리자〉란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다. 1. 5만명 이상의 정보주체에 관하여 법 23조에 따른 민감정보 or 법 24조에 따른 고유식별정보를 처리하는 자 2. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 자
		② ①항 각 호의 어느 하나에 해당하는 개인정보처리자는 서면/전화/문자전송/전자우편 등의 방법 중 어느 하나를 통하여 법 20조 ①항 각 호의 사항을 알려야 한다. 이 경우 개인정보를 제공받은 후 3개월을 경과하여서는 아니 된다.
		③ ①항 각 호의 어느 하나에 해당하는 개인정보처리자는 정보주체에게 ②항에 따라 알린 사실을(시기 및 방법을 포함한다) 해당 정보를 파기할 때까지 관리하여야 한다.

발송일
2016. 01

2015.12.31 개정

〈개인정보 영향평가에 대한 고시〉의 핵심변화는

평가영역 Ⅳ. 기술적 보호조치 신설

개인정보보호법 원문보기

평가영역 Ⅰ.
대상기관의
개인정보관리체계 (8)

1. 조직(2) 2. 계획(2)
3. 침해대응(2)
4. 정보주체권리보장(2)

평가영역 Ⅱ.
대상시스템의
개인정보관리체계 (6)

5.개인정보취급자관리(2)
6.개인정보파일관리(2)
7. 개인정보처리방침(2)

평가영역Ⅲ.
개인정보처리단계별
보호조치 (12)

8. 수집(2) 9. 보유(1)
10. 이용제공(3)
11.위탁(3) 12.파기(3)

평가영역 신설 (기존에는 평가영역3에 포함)

평가영역Ⅳ. 대상시스템의 기술적 보호조치 (20)

13. 접근권한관리(3)
14. 접근통제(3)
15. 개인정보의 암호화(2)
16. 접속기록의 보관 및 점검(3)
17. 악성프로그램 등 방지(2)
18. 물리적접근방지(2)
19. 개인정보의파기(1)
20. 기타 기술적보호조치(3)
21. 개인정보처리구역보호(1)

평가영역Ⅴ.
특정 IT기술 활용시
개인정보보호(9)

22. CCTV(4)
23. RFID(2)
24. 바이오정보(1)
25. 위치정보(2)

〈개인정보 영향평가에 대한 고시〉 내 기술적 보호조치 상세보기

평가영역 신설	평가분야	세부분야	개인정보보호법 해당조항 [개인정보의 안전성확보조치]	기술적 보호조치 예
Ⅳ. 대상 시스템의 기술적 보호조치	13. 접근권한 관리	계정/인증/권한 관리	4조 접근권한의 관리	[DB방화벽(접근통제)] DB-i
	14. 접근통제	접근통제 조치	5조 접근통제 ①②	[DB방화벽(접근통제)] DB-i
		인터넷 홈페이지 보호조치	5조 접근통제 ④	[Network DLP] Mail-i [웹서버 개인정보 유노출통제 솔루션]
		업무용 모바일 기기 보호조치	5조 접근통제 ⑥	[모바일기기내 개인정보검출 및 파기 · 암호화] SMART-i
	15. 개인정보의 암호화	저장 시 암호화	6조 개인정보의 암호화 ①③④⑥⑦	[PC] Privacy-i [서버] Server-i [모바일] SMART-i [DB암호화 솔루션]
		전송 시 암호화	6조 개인정보의 암호화 ②	[DB방화벽(접근통제)] DB-i [VPN 솔루션]
	16. 접속기록의 보관 및 점검	접속기록 보관	7조 접속기록의 보관 및 점검 ①	[DBMS 접속기록보관 및 점검] DB-i [Application 접속이력 보관 및 점검] WAS-i, App-i
		접속기록 점검	7조 접속기록의 보관 및 점검 ②	
		접속기록 보관 및 백업	7조 접속기록의 보관 및 점검 ③	
	17. 악성프로그램 등 방지	백신 설치 및 운영	8조 악성프로그램 등 방지	[악성프로그램 감염방지 세이프웹브라우징] WebKeeper [Anti-Virus]
		보안업데이트 적용		
	18. 물리적 접근방지	출입통제 절차 수립	9조 물리적 접근방지	Privacy-i 개인정보가 보조저장매체로 복제되는 것을 최소화함으로써 물리적접근방지대상 최소화효과
		반출/입 통제 절차 수립		
	19. 개인정보의 파기	안전한 파기	10조 파기	Privacy-i 복구불가능하도록 7회 이상파기
	20. 기타 기술적 보호조치	개발 환경 통제		
		개인정보 처리화면 보안		[화면캡쳐 방지] [마스킹 솔루션]
		출력 시 보호조치		Privacy-i 출력시 결재, 차단
	21. 개인정보처리 보호구역	보호구역지정		

〈개인정보 영향평가에 대한 고시〉 이외 변화 상세보기

평가영역	평가분야	세부분야	기존 대비 변화	
Ⅰ. 대상기관 개인정보보호 관리 체계	1.대상기관 개인정보 보호조직	개인정보보호책임자의 지정	〈동일〉	
		개인정보보호책임자 역할수행	〈변경〉	←(기존에는) 개인정보 보호 담당자의 지정
	2. 개인정보보호계획	내부관리계획 수립	〈변경〉	←(기존에는) 개인정보 보호 계획 수립
		개인정보보호 연간계획 수립		←(기존에는) 개인정보 보호 교육 계획 수립
	3. 개인정보 침해대응	침해사고 신고 방법 안내	〈변경〉	←(기존에는) 침해사고 처리절차
		유출사고 대응		
	4. 정보주체 권리보장	정보주체 권리보장 절차수립	〈변경〉	←(기존에는) 침해사고 처리절차
		정보주체 권리보장 방법안내		
Ⅱ. 대상시스템의 개인정보보호 관리체계	5. 개인정보 취급자 관리	개인정보 취급자 지정	〈변경〉	←(기존에는) 개인정보취급자의 지정, 분야별 책임관의 지정, 개인정보 취급자의 의무
		개인정보취급자 관리,감독		
	6. 개인정보파일 관리	개인정보파일대장 관리	〈변경〉	←(기존에는) 개인정보 파일의 안내
		개인정보파일 등록		
	7. 개인정보처리방침	개인정보처리방침의 공개	〈변경〉	←(기존에는) 일반관리 대책
		개인정보처리방침의 작성		
Ⅲ. 개인정보처리 단계별 보호조치	8. 수집	개인정보 수집의 적합성	〈변경〉	←(기존에는) 개인정보 수집의 적합성 개인정보 수집 동의의 적합성 개인정보 수집 사실의 안내 개인정보 수집 시 보호조치
		동의 받는 방법의 적절성		
	9. 보유	보유기간 산정	〈변경〉	←(기존에는) 개인정보파일보유의 적합성평가 개인정보파일대장의 작성 개인정보 저장및보유시 암호화
	10. 이용/제공	개인정보 제공의 적합성	〈변경〉	←(기존에는) 이용 및 제공의 기본원칙 타 기관 연계, 제공시 절차 개인정보처리 시스템 접근통제 웹 및 애플리케이션 통제 개인정보 처리 단말기 보호조치 개인정보 이용/제공승인 네트워크 접속통제 웹사이트 개인정보 노출차단 개인정보 처리내역 기록관리
		목적 외 이용/제공 제한		
		제공시 안전성 확보		
	11. 위탁	위탁사실 공개	**〈신설〉**	
		위탁 계약		
		수탁사 관리/감독		
	12. 파기	파기계획수립	〈변경〉	←(기존에는) 보유기간 산정 및 안내
		분리보관 계획수립		
		파기대장 작성		
Ⅴ. 특정 IT기술 활용시 개인정보보호	22. CCTV	CCTV 설치시 의견수렴	〈동일〉	
		CCTV 설치 안내		
		CCTV 사용 제한		
		CCTV 설치 및 관리에 대한 위탁		
	23. RFID	RFID 이용자 안내		
		RFID 태그부착 및 제거		
	24. 바이오정보	원본정보 보관 시 보호조치		
	25. 위치정보	개인위치정보 수집 동의		
		개인위치정보 제공 시 안내사항		

발송일
2015. 10

2015.10.7일부터 11.27일까지

행정자치부, 전국 15,751개 공공기관 대상(초중고교 포함)
11,249개 개인정보처리시스템 일제점검

개인정보처리시스템 일제점검 원문보기

지금 무엇을 준비해야 하는가?

모든 공공기관

개인정보처리시스템 내 접근통제 및 기록관리여부 체크

개인정보 사적조회 및 3자 제공, 금품수수 등 개인정보 오남용 예방

수탁사 성격 공공기관

행정자치부 11월 현장점검 사전대비

사고 발생 우려가 있는 대량 개인정보 보유기관 집중점검

대상 15,751개 공공기관(초중고교 포함) 의 11,249개 개인정보처리시스템

일시 2015.10.7~11.27

주관 행정자치부, 한국인터넷진흥원

진행절차

행정자치부
15,751개 공공기관에 〈개인정보처리시스템 자율점검표〉 배포

▶

15,751개 공공기관
10.27일까지 〈개인정보처리시스템 자율점검표〉 35개 항목으로 자체점검 실시 및 점검결과 〈자율점검 홈페이지〉에 등록

▶

중앙행정기관, 광역자치단체
11월, 소관 취약기관 및 미실시기관 확인점검

▶

행정자치부, 한국인터넷진흥원
11.16~27일, 취약기관 및 수탁사 성격 기관 현장점검

▶

행정자치부
11.27일 이후, 점검결과 및 내용 〈자율점검 홈페이지〉 등록

▶

행정자치부
향후 공공기간 대상
연 3회이상 기획점검 실시
연 1회 자율점검 실시

〈자율점검표〉 구성

정책수립 5개 항목
개인정보보호법 29조, 30조, 31조 기반

▶

기술적 보호조치 15개 항목
개인정보보호법 29조 기반

▶

수집 4개 항목
개인정보보호법 15조, 22조, 23조, 24조 기반

▶

이용자 권리보호 7개항목
개인정보보호법 17조, 22조, 26조 기반

▶

보유, 파기 5개 항목
개인정보보호법 21조, 32조 기반

〈개인정보처리시스템 자율점검표〉 35개 항목 보기 1/2

개선이 필요하다면?

개 인정보보호법

개	세부확인사항	YES	NO	N/A	기술적 보호조치
31조	1. 개인정보보호책임자 지정		✓		
29조	2. 개인정보의 안전한 처리를 위한 내부관리계획 수립		✓		
30조	3. 개인정보처리방침 공개		✓		
	4. 개인정보처리방침내용(처리 및 보유기간, 위탁사항)의 적절성		✓		
	5. 개인정보처리방침 변경 내용 지속적 공개 및 이력관리		✓		
29조	6. 개인정보처리시스템 · 업무용컴퓨터 내 백신소프트웨어 설치 · 운영		✓		[바이러스솔루션]
	7. 침입 차단(F/W) · 방지(IPS) · 탐지(IDS) 등 접근통제시스템 설치 · 운영		✓		[DB] DB-i [WAS] WAS-i [SAP] APP-i
	8. 개인정보처리시스템의 중요도(민감도) 및 업무연관성 등을 고려한 담당자별 차등 접근권한 절차 마련		✓		
	9. 전보 또는 퇴직 인력의 개인정보처리시스템 접근권한 즉시 삭제		✓		
	10. 접근권한 부여 · 변경 · 말소에 대한 이력관리 수행		✓		
	11. 비밀번호 작성규칙을 수립하여 개인정보처리시스템에 적용		✓		
	12. 개인정보처리시스템에 대한 외부망 접근통제 실시		✓		[DB] DB-i [WAS] WAS-i [SAP] APP-i
	13. 비인가된 P2P, 웹하드, 공개된 무선망 등 공유설정 차단		✓		[PC] Privacy-i [네트워크] Mail-i Mail-i for WebDLP
	14. 전산실, 자료보관실 등 개인정보 취급공간 출입통제절차 수립 · 운영		✓		Privacy-i 개인정보가보조저장매체, 서류로복제되는 것을 최소화함으로써 물리적 접근방지대상 최소화
	15. 고유식별정보(주민등록번호, 여권번호 등) 암호화 저장		✓		[DB] DB암호화 [PC] Privacy-i DRM
	16. 비밀번호는 일방향 암호화 저장		✓		
	17. 고유식별정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 송 · 수신 시 암호화 전달		✓		보안서버 (SSL외) [DB] DB-i [보조저장매체] Privacy-i
	18. 개인정보처리시스템 접속기록 6개월 이상 보관 · 관리		✓		[DB] DB-i [WAS] WAS-i [SAP] APP-i
	19. 개인정보처리시스템 접속기록이 위 · 변조 및 도난, 분실되지 않도록 안전하게 보관		✓		
	20. 개인정보처리시스템 접속기록점검 및 후속조치 반기별 1회 이상		✓		

기술적 보호조치 15개 항목

〈개인정보처리시스템 자율점검표〉 35개 항목 보기 2/2

개 인정보보호법

개선이 필요하다면?

개	세부확인사항	YES	NO	N/A	기술적 보호조치
15조	21. 개인정보 수집시(회원가입, 게시판 등), 정보주체의 동의를 받고 있는지 여부		✓		
23조 24조	22. ① 민감/고유식별정보(주민번호 제외) 수집시 별도 개인정보주체 동의 or 법령에 근거하여 수집 ② 주민번호 수집시 법률에 근거하여 수집		✓		
22조	23. 만14세 미만 아동 개인정보 수집시 법정대리인 동의를 받고 있는지 여부		✓		
15조	24. 개인정보 수집 시, 필수 고지항목(4개)을 명확하게 고지하는지 여부 ① 개인정보의 수집 · 이용 목적 ② 수집하려는 개인정보의 항목 ③ 개인정보의 보유 및 이용 기간 ④ 동의 거부 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용		✓		
22조	25. 홍보 활용 정보와 그렇지 않은 정보를 구분하여 동의를 받고 있는지 여부		✓		
	26. 선택항목 및 홍보권유 정보 미동의시 재화 또는 서비스 제공 거부를 하지 않는지 여부		✓		
17조	27. 제3자 제공에 관한 사항을 정보주체에게 알리고 동의를 받는지 여부		✓		
	28. 제3자 제공에 관한 동의시 필수고지항목(5개)을 명확하게 고지하는지 여부 ① 개인정보를 제공받는 자 ② 개인정보를 제공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 ⑤ 동의 거부 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용		✓		
26조	29. 개인정보의 처리 업무 위탁 시, 문서(계약서 등)에 의한 것인지 여부		✓		
	30. 위탁업무의 내용과 수탁자(위탁받아 처리하는 자) 공개		✓		
21조	31. 개인정보 처리목적 달성시 지체 없이 파기		✓		[PC] Privacy-i [서버] Server-i
	32. 다른 법령에 따라 개인정보 미파기 및 보존시 다른 개인정보와 분리저장 · 관리		✓		
32조	33. 개인정보파일 운용시 개인정보보호종합지원시스템(intra.privacy.go.kr) 등록		✓		
	34. 개인정보파일 보유기간이 타당한지 여부		✓		[PC] Privacy-i [서버] Server-i
	35. 개인정보파일 불필요 시 지체없이 파기		✓		

개인정보보호법 고시 개정안
Privacy Report 보기

02

정보통신망법

(적용대상 : 정보통신서비스 제공자)

2016년 개정,정보통신망법 변화

정보통신망법고시
〈개인정보의 기술적 관리적 보호조치 기준〉 강화

① 정보통신망법고시 위반으로 유출 발생시 처벌 강화

이전 Report 보기

징벌적
손해배상
(시행일 2016.7.25)
32조 ②항

법 위반 사실 인지시
CPO→CEO 보고
27조

법 위반시
방통위가 CEO, 임원 징계
69조의2

위반행위 관련
취득한 금품,
그 밖의 이익은
몰수 or 가액 추징
75조의2

법 위반시 미래부or 방통위 공무원이 사업장에 출입하여 감사가능
64조

② 정보통신망법고시 규정 중 〈점검→파기〉 강화

이전 Report 보기

웹사이트에 노출된
개인정보 파기 차단
(시행일 2016.7.25)
32조의3

법 위반 사실 인지시
CPO→CEO 보고
27조

법 위반시
방통위가 CEO, 임원 징계
69조의2

위반행위 관련
취득한 금품,
그 밖의 이익은
몰수 or 가액 추징
75조의2

법 위반시 미래부or 방통위 공무원이 사업장에 출입하여 감사가능
64조

③ 그 외 변화들

이전 Report 보기

스마트폰앱 내 개인정보 접근통제
(시행일 2017.3.22)
22조의2

개인정보처리의
범위확대
24조의2

취급위탁
규정 강화
25조

정보통신망을 통하여
개인정보 거래금지
44조의7

(피싱or 파밍 등) 속이는 행위로 개인정보수집발생시 이용자에게
안내메시지를 보낼 수있는 시스템 구축 (2016. 9.22 이내 완료)
49조의2, 부칙3조

(동의받아야 하는) 개인정보 해외이전 개념구체화
→제공(조회 포함), 처리위탁, 보관
63조 ②항

정보통신망 해킹미수범도 처벌
→5년이하 징역 or 5천만원이하 벌금
71조

악성프로그램 유포자 처벌강화
→7년이하 징역 or 7천만원이하 벌금
70조의2

용어변경 및 통일
→취급을 처리로 용어변경

발송일
2015. 05

2015년 5월 19일, 오늘부터 시행됩니다!

정보통신망법고시 〈개인정보의 기술적 관리적 보호조치 기준〉 개정시행

정보통신망법고시 개정시행 원문 보기

2012년 8월(고시 제2012-50호) 이후 최초의 대대적 개정, 무엇이 바뀌나?

개 정 방 향	개 정 내 용
유출사고 관련규정 추가 1. 대형유출사고 재발방지규정 2. 유출발생시 대처규정 신설 3. 위탁자 관리감독책임 확대	**위탁자의 수탁자 관리감독책임 확대** (2014년 카드사유출 재발방지) 일부삭제 2조 2호 〈개인정보취급자의 정의〉 ~~정보통신서비스제공자 사업장내에서~~ 이용자 개인정보를 수집,보관,처리, 이용,제공,관리,파기하는 자 일부삭제 2조 1호 〈개인정보관리책임자의 정의〉 ~~정보통신서비스제공자 사업장내에서~~ 이용자 개인정보보호업무를 총괄 or 최종결정하는 임직원 신설 3조 ①항 〈조직구성시 반영사항〉 5. 개인정보 처리업무 위탁시 수탁자 관리감독 공간적 제한 삭제 **접속시간제한** (2011년 정보통신권유출 재발방지) 신설 4조 ⑩항 개인정보취급자 접속은 필요시간내에서 유지되도록 최대 접속시간 제한 **유출시 대응이 개인정보보호조직 주요업무로 등장** 신설 3조 ①항 6호 〈조직구성시 반영사항〉 유출사고 등 발생시 대응절차 및 방법
기업규모에 따라 보호수준이 상승해야 함을 명시 고시는 소규모사업자에게도 적용되는 최소기준 구체적 보호조치예 삭제	변경 1조 ①항〈목적〉 개인정보 안전성 확보에 필요한 기술적 관리적 보호조치 (구체적 →) 최소기준 설정 신설 1조 ②항〈목적〉 사업규모, 개인정보보유수에 비례하는 개인정보보호조치기준 수립, 시행 변경 3조 ②항 책임자/취급자대상 개인정보교육 (매년 2회 이상 →) 사업규모/개인정보 보유 수를 고려하여 정기적으로 실시 일부삭제 4조 ④항 개인정보처리시스템 외부접속시 ~~공인인증서 등~~ 안전한 인증수단 적용 변경 4조 ⑧항 취급자대상 비밀번호 작성규칙 수립 (영문 대문자/소문자 →) 영문/숫자/특수문자 중 조합 일부삭제 10조 개인정보조회/출력시 마스킹 원칙 삭제 ~~1. 이름 첫글자 2. 생년월일 3. 전화국번 4. 주소 읍/면/동 5. 인터넷주소~~
개인정보보호법 고시와의 정합성 확보	신설 2조 13호 〈모바일기기의 정의〉 모바일기기란 스마트폰, 태블릿PC 등 무선망사용 휴대용 기기 추가 4조 ⑨항 홈페이지, P2P, 공유설정 등을 통해 개인정보가 공개/유출되지 않도록 개인정보처리시스템 및 취급자의 컴퓨터/모바일기기에 조치 추가 6조 ④항 컴퓨터/모바일기기 등에 개인정보 저장시 암호화 **암호화대상 확대** 일부삭제 6조 ①항 ~~바이오정보~~, 비밀번호는 일방향 암호화저장 추가 6조 ②항 고유식별정보(주민/여권/운전면허/외국인번호), 신용카드, 계좌번호, 바이오정보는 안전한 암호알고리즘으로 암호화저장 **물리적 접근통제규정 신설** 신설 8조 ①항 개인정보 보관장소(전산실/자료보관실) 출입통제절차 수립/운영 신설 8조 ②항 개인정보포함 서류/저장매체는 잠금장치가 있는 장소에 보관 신설 8조 ③항 개인정보포함 저장매체 반출입통제를 위한 보안대책마련

〈개인정보의 기술적 관리적 보호조치 기준〉 고시 상세규정보기 1/4

〈관리적 보호조치 기준〉

조	내용	기존과 달라진 점	관리적 보호조치
1조 목적	① 법 28조 ① 및 시행령 15조 ⑥에 따라 정보통신서비스 제공자 등 (법 67조에 따라 준용되는 자 포함)이 이용자 개인정보취급에 있어 개인정보가 분실/도난/누출/변조/훼손되지 않도록 안전성확보를 위한 기술적 관리적 보호조치 최소한의 기준을 정함	**추가** 법 67조에 따라 준용되는 자 : 지상파/종합유선/위성 /공동체라디오방송 사업자 **변경** 구체적인 기준 → 최소한의 기준	Privacy Consulting
	② 사업규모, 개인정보 보유 수 등을 고려하여 환경에 맞는 개인정보 보호조치기준 수립/시행	**신설**	
2조 정의 (총 14개 용어정의)	개인정보처리시스템 (방통위 안내서에 따라 WAS, SAP 등의 어플리케이션을 포함함) **방송통신위원회** 개인정보처리시스템에 중계서버, **어플리케이션** 등도 포함시키는 것이 타당하다 (정보통신서비스제공자 등을 위한 외부인터넷망 차단조치 안내서, 1-3, 용어의 정의, 2013.2)		
	개인정보관리책임자 (~~정보통신서비스제공자 사업장내에서~~ 이용자 개인정보 보호업무를 총괄 or 최종결정하는 임직원) 개인정보취급자 (~~정보통신서비스제공자 사업장내에서~~ 이용자 개인정보를 수집,보관,처리,이용,제공,관리,파기하는 자)	**삭제** 〈정보통신서비스 제공자의 사업장내에서〉 라는 공간적 제한 삭제	
	모바일기기(스마트폰, 태블릿PC 등 무선망사용 휴대용 기기) 보조저장매체 (이동형 하드디스크, USB, CD 등 개인정보처리시스템 or PC와 쉽게 분리접속 가능한 저장매체)	**신설** 모바일기기/보조저장매체	
	내부관리계획, 개인정보처리시스템, 망분리, 비밀번호, 접속기록, 바이오정보, P2P, 공유설정, 보안서버, 인증정보		
3조 내부관리 계획의 수립 · 시행	① 개인정보보호조직 구성/운영시 반영사항 1. 개인정보관리책임자 자격요건 및 지정 2. 개인정보관리책임자/개인정보취급자 역할 및 책임 3. 개인정보 내부관리계획 수립 및 승인 4. 개인정보의 기술적 관리적 보호조치 이행여부 내부점검 5. 개인정보처리업무 위탁시 수탁자 관리 및 감독 6. 개인정보의 ~~분실/도난/누출/변조/훼손~~ (입법예고 후 삭제) 유출사고 등 발생시 대응절차 및 방법 (입법예고 후 추가) 7. 그 밖에 개인정보보호를 위해 필요한 사항	**신설** 5. 위수탁자관리감독 6. 개인정보유출시 대응이 개인정보보호조직의 주요업무로 등장	Privacy Consulting
	② 다음 사항을 정하여 개인정보관리책임자/취급자대상 사업규모, 개인정보 보유수 등을 고려하여 (입법예고 후 추가) 정기적으로 교육실시 1. 교육목적/대상 2. 교육내용 3. 교육일정/방법	**변경** 매년 2회 이상 → 사업규모, 개인정보 보유수 등을 고려하여 정기적으로	

〈개인정보의 기술적 관리적 보호조치 기준〉 고시 상세규정보기 2/4

〈기술적 보호조치 기준〉 1/3

조	내용	기존과 달라진 점	개보법고시와의 차이	기술적 보호조치
4조 접근통제	① 〈개인정보처리시스템〉 접근권한을 개인정보관리책임자/취급자에게만 부여			[DB]DB-i [WAS]WAS-i [SAP] App-i
	② 인사이동시 지체없이 〈개인정보처리시스템〉 접근권한 변경/말소			
	③ ①,②에 의한 권한부여/변경/말소내역 최소 5년 보관		4조 ③항 최소 3년보관	
	④ 개인정보취급자가 외부에서 〈개인정보처리시스템〉에 접속할 경우 공인인증서 등 안전한 인증수단 적용	일부삭제 공인인증서		[보안토큰] [휴대폰인증] [일회용 비밀번호] [바이오정보]
	⑤ 불법접근/침해사고방지를 위해 다음 기능포함 시스템 설치운영 1. 개인정보처리시스템 접속권한을 IP주소 등으로 제한, 인가받지 않은 접근제한 2. 개인정보처리시스템 접속 IP주소 등 재분석, 불법유출시도탐지		5조 ①항과 동일	[DB]DB-i [WAS]WAS-i [SAP] App-i
	⑥ 전년도말 기준 직전 3개월간 개인정보가 저장/관리되는 이용자수가 일평균 100만명 이상 or 정보통신서비스부문 전년 매출액 100억원 이상인 정보통신서비스 제공자 등은 개인정보 다운로드/파기/접근권한설정 가능한 개인정보취급자 컴퓨터 등을 물리적 or 논리적으로 망분리	추가 대통령 규정을 고시에도 명시	규정없음	[망분리솔루션]
	⑦ 이용자가 안전한 비밀번호를 이용할 수 있도록 비밀번호작성규칙 수립/이행		규정없음	Privacy Consulting
	⑧ 개인정보취급자대상 비밀번호 작성규칙 수립/적용/운용 1. 영문/숫자/특수문자 2종류이상 조합시 최소 10자리 이상 3종류이상 조합시 최소 8자리 이상 2. 추측하기 쉬운 개인정보(생일, 전화번호), 아이디와 비슷한 비밀번호는 사용하지 않을 것 3. 반기별 1회 이상 변경	변경 영문 대문자/소문자 → 영문	4조 ⑤항 고시규정이 아니라 해설서상에 행정지도로 존재	
	⑨ 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 공개/유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터/모바일기기에 조치	추가 모바일기기	5조 ④항 개인정보처리시스템 컴퓨터, 모바일기기 + 공개된 무선망	[Network DLP] Mail-i [Endpoint DLP] Privacy-i [모바일] Smart-i
	⑩ 개인정보취급자 접속이 필요시간 내에서만 유지되도록 최대 접속시간제한 등 조치	신설	규정없음	[DB]DB-i [WAS]WAS-i [SAP] App-i 최대접속시간 제한 심야/휴일접속 차단

〈개인정보의 기술적 관리적 보호조치 기준〉 고시 상세규정보기 3/4

〈기술적 보호조치 기준〉 2/3

조	내용	기존과 달라진 점	개보법 고시와의 차이	기술적 보호조치
5조 접속기록의 위변조방지	① 개인정보처리시스템 접속기록 월 1회이상 확인감독 최소 6개월 이상 접속기록 보존/관리		7조 ②항 반기별 1회이상 점검	[DB]DB-i [WAS]WAS-i [SAP] App-i
	② 기간통신사업자는 최소 2년 보존		규정없음	
	③ 접속기록이 위변조되지 않도록 별도의 물리적인 저장장치에 보관, 정기적백업 수행		7조 ③항과 동일	
6조 개인정보의 암호화	① 비밀번호 및 ~~바이오정보는~~ 일방향 암호저장	일부삭제 바이오정보 → ②항으로 이동	6조 ③항과 동일	[PC] Privacy-i [서버] Server-i [모바일] Smart-i
	② 다음사항은 안전한 암호알고리즘으로 암호화저장 1. 주민번호 2. 여권번호 3. 운전면허번호 4. 외국인등록번호 5. 신용카드번호 6. 계좌번호 7. 바이오정보	추가 여권번호/ 운전면허번호/ 외국인등록번호/ 바이오정보	6조 ①항 신용카드번호, 계좌번호 미포함	
	③ 이용자 개인정보/인증정보 송수신시 암호화, 보안서버는 다음 중 하나의 기능을 갖추어야 함 1. 웹서버에 SSL인증서 설치, 전송정보 암호화 2. 웹서버에 암호화 응용프로그램 설치, 전송정보 암호화		규정없음	
	④ 이용자 개인정보를 컴퓨터, 모바일기기 및 보조저장매체 등에 저장시 암호화	추가 모바일기기/ 보조저장매체	6조 ⑦항과 동일	
7조 악성 프로그램 방지	· 백신SW 일 1회 이상 주기적으로 갱신/점검 · 악성프로그램관련 경보 or 백신SW/OS업체 업데이트 공지시 최신 SW로 즉시 갱신/점검	변화 월 1회→일 1회 추가 즉시	8조와 동일	[세이프브라우징] WebKeeper [치료] 백신 [패치관리SW]
8조 물리적 접근방지	① 전산실/자료보관실 등 개인정보 보관장소 출입통제절차 수립/운영	신설	9조와 동일	Privacy-i 개인정보가 보조저장매체/ 서류로 복제되는 것을 최소화하여 물리접근 방지대상 최소화
	② 개인정보포함 서류/저장매체는 잠금장치가 있는 장소에 보관			
	③ 개인정보포함 저장매체의 반출입 통제를 위한 보안대책 마련			
9조 출력복사시 보호조치	① 개인정보출력시(인쇄, 화면표시, 파일생성 등) 용도특정/출력항목 최소화		규정없음	[Endpoint DLP] Privacy-i 출력물, 외부저장매체 복제시 기록/차단
	② 개인정보포함 인쇄물/외부저장매체 안전관리를 위한 출력/복사기록 등 필요한 보호조치 구축			
제10조 개인정보 표시제한 보호조치	개인정보조회/출력 등 업무수행시 개인정보 마스킹 [마스킹시 적용가능한 원칙] ~~1. 이름 첫글자 2. 생년월일~~ ~~3. 전화국번 4. 주소 읍·면·동~~ ~~5. 인터넷주소는 버전4 경우 17~24비트영역,~~ ~~버전 6 경우 113~128비트 영역~~	일부삭제 이름 첫글자/ 생년월일/전화 국번/주소/ 인터넷주소	10조 ②항 개인정보 일부파기시 마스킹으로 대체 규정있음	[개인정보마스킹] DB-i Privacy-i

〈개인정보의 기술적 관리적 보호조치 기준〉 고시 상세규정보기 4/4

〈기술적 보호조치 기준〉 3/3

조	내용	기존과 달라진 점	개보법 고시와의 차이	기술적 보호조치
8조 물리적 접근방지	① 전산실/자료보관실 등 개인정보 보관장소 출입통제절차 수립/운영	신설	9조와 동일	Privacy-i 개인정보가 보조저장매체/서류로 복제되는 것을 최소화하여 물리접근 방지대상 최소화
	② 개인정보포함 서류/저장매체는 잠금장치가 있는 장소에 보관			
	③ 개인정보포함 저장매체의 반출입 통제를 위한 보안대책 마련			
9조 출력복사시 보호조치	① 개인정보출력시(인쇄, 화면표시, 파일생성 등) 용도특정/출력항목 최소화		규정없음	[Endpoint DLP] Privacy-i 출력물, 외부저장매체 복제시 기록/차단
	② 개인정보포함 인쇄물/외부저장매체 안전관리를 위한 출력/복사기록 등 필요한 보호조치 구축			
제10조 개인정보 표시제한 보호조치	개인정보조회/출력 등 업무수행시 개인정보 마스킹 [마스킹시 적용가능한 원칙] ~~1. 이름 첫글자~~ ~~2. 생년월일~~ ~~3. 전화국번~~ ~~4. 주소 읍·면·동~~ ~~5. 인터넷주소는 버전4 경우 17~24비트영역,~~ ~~버전 6 경우 113~128비트 영역~~	일부삭제 이름 첫글자/생년월일/전화국번/주소/인터넷주소	10조 ②항 개인정보 일부파기시 마스킹으로 대체 규정있음	[개인정보마스킹] DB-i Privacy-i

발송일
2016. 03

3.22일 공포, 9.23일 시행 **2016년 개정, 정보통신망법 핵심변화 ①**

정보통신망법고시 〈개인정보의 기술적 관리적 보호조치 기준〉 위반 → 유출시 처벌강화

정보통신망법고시 개정안 원문 보기

〈고시 위반시 처벌〉

기존 과징금

위반행위 관련
매출의 3%까지 징수

73조

이전 Report 보기

+

개정 위반시 징계대상자로 CEO 명시

법 위반사실 인지시 CPO는 즉시 개선조치 시행→CEO에게 보고	법 위반시 방통위가 CEO, 임원 징계
27조	69조의2

2014.7월 〈개인정보보호 정상화대책〉에서 개정예고

개정 위반시 미래부or 방통위 공무원이 사업장에 출입하여 감사가능 64조

이전 Report 보기

〈고시 위반으로 유출시 처벌〉

기존 검찰고발

접근통제, 접속기록위변조방지, 전송저장시암호화, 악성코드침해 방지조치를 하지않아 개인정보유출시 방통위가 검찰에 유출사업자 고발 69조의2

이전 Report 보기

기존 형사처벌

2년 이하 징역 or 2천만원 이하 벌금

64조의3 ①항 6호 ,73조 1호

이전 Report 보기

개정

고시 위반으로 취득한 금품, 그 밖의 이익은 몰수 or 가액 추징 32조

* 가액(價額): 물건 가치에 상당한 금액

+

개정 고객의 피해입증이 가능한 경우
〈징벌적 손해배상〉 1인당 피해액의 3배까지 배상 (2016.7.25시행)

정보통신망법 32조 ②
고의 or 중대한 과실로 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 or 훼손되어 이용자에게 손해가 발생한 때 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다.
* 예외: 고의 or 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다.

2014.7
국무총리실 범정부TF
〈개인정보보호 정상화대책〉에서
개정예고 이전 Report 보기

손해배상 청구절차는

개인정보 유출 사고 발생

개정 피해입증이 가능한 고객은 〈징벌적 손해배상〉청구

기존 피해입증이 불가능한 고객은 〈법정 손해배상〉청구

기업
고의 · 과실이 없었음을 입증
입증 못하면 배상

고시를 100% 준수했음을 입증해야 함

개정 법원, 피해액의 3배 내에서 배상액 산정

기존 법원, 300만원 내에서 배상액 산정

법원의 배상액 산정시 고려사항	
위반행위로 인한 혹은 위반행위의	피해 규모
	〈서비스 제공자〉가 취득한 경제적 이익
	벌금 및 과징금
	기간 · 횟수 등
〈서비스 제공자〉의	재산상태
	고의 or 손해발생의 우려를 인식한 정도
〈서비스 제공자〉가	개인정보 분실 · 도난 · 유출 후 해당 개인정보 회수를 위해 노력한 정도
	이용자의 피해구제에 노력한 정도

〈고시위반 → 유출〉 관련 상세규정 보기

<table>
<tr><th>조항</th><th>개정여부</th><th>내용</th></tr>
<tr><td>27조</td><td>신설</td><td>④ CPO는 이 법 및 다른 관계 법령 위반사실을 알게 된 경우,
즉시 개선조치를 하고 필요시 사업주 or 대표자에게 개선조치 보고</td></tr>
<tr><td>32조</td><td>신설</td><td>② 고의 or 중대한 과실로 개인정보가
분실 · 도난 · 유출 · 위조 · 변조 or 훼손되어
이용자에게 손해가 발생한 때 법원은
그 손해액의 3배를 넘지 아니하는 범위에서
손해배상액을 정할 수 있다.
*예외: 고의 or 중대한 과실이 없음을
증명한 경우에는 그러하지 아니하다.
<table>
<tr><th colspan="2">법원의 배상액 산정시 고려사항</th></tr>
<tr><td rowspan="4">위반행위로 인한 혹은 위반행위의</td><td>피해 규모</td></tr>
<tr><td>〈서비스 제공자〉가 취득한 경제적 이익</td></tr>
<tr><td>벌금 및 과징금</td></tr>
<tr><td>기간 · 횟수 등</td></tr>
<tr><td rowspan="2">〈서비스 제공자〉의</td><td>재산상태</td></tr>
<tr><td>고의 or 손해발생의 우려를 인식한 정도</td></tr>
<tr><td rowspan="2">〈서비스 제공자〉가</td><td>개인정보 분실 · 도난 · 유출 후 해당 개인정보회수를 위해 노력한 정도</td></tr>
<tr><td>이용자의 피해구제에 노력한 정도</td></tr>
</table></td></tr>
<tr><td rowspan="3">64조</td><td>기존</td><td>① 다음 경우 미래부 or 방통위는 관계 물품 · 서류 등을 제출 요구할 수 있다
1. 법위반사항을 발견 or 혐의를 알게 된 경우 2. 이 법의 위반에 대한 신고를 받거나 민원이 접수된 경우
2의2. 이용자 정보의 안전성과 신뢰성 확보를 현저히 해치는 사건 · 사고 등이 발생하였거나 발생할 가능성이 있는 경우</td></tr>
<tr><td>기존</td><td>② 방통위는 (이 법을 위반, 영리목적 광고성 정보를 전송한 자에게 조치를 하기 위하여)
해당 광고성 정보 전송자의 성명 · 주소 · 주민등록번호 · 이용기간 등에 대한 자료의 열람이나 제출을 요청할 수 있다.</td></tr>
<tr><td>개정</td><td>③ 미래부 or 방통위는 〈정보통신서비스제공자〉가 ① 및 ②에 따른 자료를 제출하지 아니하거나
이 법을 위반한 사실이 있다고 인정되면 소속공무원에게 정보통신서비스 제공자등, 해당 법 위반 사실과 관련한 관계인의 사업장에 출입하여 업무상황, 장부 or 서류 등을 검사하도록 할 수 있다.</td></tr>
<tr><td rowspan="2">69조
의2</td><td>기존</td><td>① 방통위는 다음 〈정보통신서비스제공자〉를 검찰 등 수사기관에 고발할 수 있다.
6. 이용자의 개인정보를 분실 · 도난 · 누출 · 변조 또는 훼손한 경우로서 28조 ①항의 2~5호까지 조치를 하지 아니한 경우
* 28조 ①
2. 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치 · 운영
3. 접속기록의 위조 · 변조 방지를 위한 조치 4. 안전하게 저장 · 전송할 수 있는 암호화기술 등을 이용한 보안조치
5. 백신 소프트웨어의 설치 · 운영 등 컴퓨터바이러스에 의한 침해 방지조치</td></tr>
<tr><td>신설</td><td>② 방통위는 이 법을 위반한 〈정보통신서비스제공자〉에게 책임있는 자(대표자 및 책임있는 임원을 포함한다)를 징계할 것을 권고할 수 있다. 이 경우 이를 존중하여야 하며 그 결과를 방통위에 통보하여야 한다.</td></tr>
<tr><td>75조
의2</td><td>신설</td><td>
<table>
<tr><th>조항</th><th colspan="2">내용</th><th>처벌</th></tr>
<tr><td rowspan="8">71조</td><td rowspan="4">이용자의 동의를 받지 아니하고</td><td>① 개인정보를 수집한 자</td><td rowspan="8">5년이하 징역
or
5천만원 이하 벌금</td></tr>
<tr><td>② 개인의 권리/이익, 사생활을 침해할 우려가 있는 개인정보를 수집한 자</td></tr>
<tr><td>③ 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 or 부정한 목적으로 개인정보를 제공받은 자</td></tr>
<tr><td>④ 개인정보 취급위탁을 한 자</td></tr>
<tr><td colspan="2">⑤ 이용자의 개인정보를 훼손/침해 or 누설한 자</td></tr>
<tr><td colspan="2">⑥ 개인정보가 누설된 사정을 알면서도 영리 or 부정한 목적으로 개인정보를 제공받은 자</td></tr>
<tr><td colspan="2">⑦ (이용자가 정정요구한 경우에도) 필요한 조치 없이 개인정보를 제공하거나 이용한 자</td></tr>
<tr><td colspan="2">⑧ 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 자</td></tr>
<tr><td>72조</td><td colspan="2">② (정보통신망을 통하여 속이는 행위로) 다른 사람의 개인정보를 수집한 자 (49조 ①)</td><td>3년이하 징역
or
3천만원 이하 벌금</td></tr>
<tr><td rowspan="3">73조</td><td colspan="2">① (정보통신망법고시 〈개인정보의 기술적 관리적 보호조치 기준〉 위반으로)
기술적 · 관리적 조치를 하지 아니하여 이용자의 개인정보를 분실/도난/누출/변조 or 훼손한 자</td><td rowspan="3">2년이하 징역
or
2천만원 이하 벌금</td></tr>
<tr><td colspan="2">①의2. (보유이용기간이 종료된 경우 복구재생되지않는 방법으로) 개인정보를 파기하지 아니한 자</td></tr>
<tr><td colspan="2">⑦ (정보통신망을 통하여 속이는 행위로) 개인정보의 제공을 유인한 자</td></tr>
</table>
+ 몰수, 추징
해당 위반행위와 관련하여 취득한 금품이나 그 밖의 이익은 몰수할 수 있으며, 불가능할 경우 그 가액을 추징할 수 있다.
</td></tr>
</table>

발송일
2016. 03

3.22일 공포, 9.23일 시행 2016년 개정, 정보통신망법 핵심변화 ②

개인정보〈미점검→미파기〉 시 처벌강화

정보통신망법 개정안 원문 보기

기존 개인정보 〈미점검→미파기〉시 처벌

〈점검→파기〉하지 않으면 범죄!
유출되지 않더라도 유출과 동일한 형사처벌 가능

정보통신망법 29조 ① (보유이용기간 끝난 개인정보의 파기)
개인정보 보유,이용기간이 끝났거나 수집이용목적이 달성되면 복구/재생할수 없도록 파기해야 한다

정보통신망법 73조 1의2호 (벌칙)
(정보통신망법 29조 1항을 위반하여) 개인정보를 파기하지 아니한 자를 2년 이하 징역 or 2천만원 이하 벌금에 처한다

형사처벌
개인정보 미파기시
2년 이하 징역 or
2천만원 이하 벌금
정보통신망법 73조 1의2호
이전 Report 보기

과태료
〈휴면기간(1년) 종료된 개인정보〉
미파기시
3천만원 이하 과태료
정보통신망법 29조 ②항
이전 Report 보기

과태료
〈개인정보취급방침〉에
파기절차/방법 미공개시
3천만원 이하 과태료
정보통신망법 27조의2
이전 Report 보기

신설&개정 개인정보〈미점검→미파기〉시 처벌 강화

신설
〈미점검→미파기〉로 취득한
금품, 그 밖의 이익은
몰수 or 가액 추징
(다른 벌칙에 부가하여 과할 수 있다)
정보통신망법 32조

신설
웹사이트에 개인정보 (특히 주민, 카드, 계좌)가 노출되지 않도록 조치
방통위or KISA가 삭제/차단요청할 경우 따라야 함
위반시 3천만원 이하 과태료
정보통신망법 32조의3

신설
위반시 징계대상자로 CEO 명시
법 위반 사실 인지시 CPO는 즉시 개선조치 →CEO에게 보고
정보통신망법 27조
법 위반시 방통위가 CEO, 임원 징계
정보통신망법 69조의2
2014.7 〈개인정보보호 정상화대책〉에서 개정예고
이전 Report 보기

개정
위반시
미래부or 방통위 공무원이
사업장에 출입하여 감사가능
정보통신망법 64조

개인정보 미파기죄는 양벌규정이 적용되므로 〈CEO 리스크〉임

정보통신망법 75조 (양벌규정)

② 법인의 대표자나 법인의 대리인, 사용인, 종업원이 그 법인 or 개인의 업무에 관하여 71조, 72조, 74조①, **73조의 위반행위를 하면** 행위자를 벌하는 외에 법인에게도 벌금형을 과(科)한다

BUT

법인이 위반행위 방지를 위하여 **상당한 주의와 감독**을 한 경우 **처벌하지 않는다**

73조 1의2호〈개인정보 미파기〉발생시

위반 행위의 〈행위자〉식별

직원 or 외주직원의 고의/과실이 원인일 때

2014년 이후 법의 판단은 CEO의 책임강화로 이동

CEO 결재 책임사항으로 CEO의 법규위반이 원인일 때

법인의 〈상당한 주의와 감독〉 여부판단

법인이 〈선량한 관리자의 의무〉를 준수했는지 판단

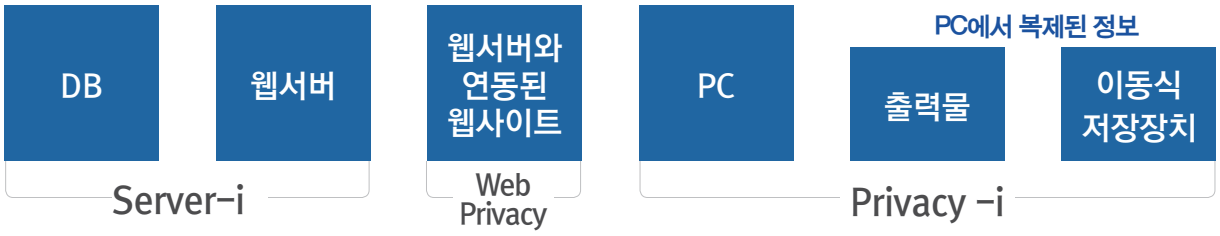
- 법규를 준수했는가?
- 〈기존 판례상 명시된 과실〉이 재발하는 것을 방지했는가?
- 기술적 보호수준이 동종업계 평균 이상인가?

〈행위자〉, 〈법인〉 처벌

행위자처벌	법인처벌	행위자처벌	법인처벌
직원 or 외주직원 형사처벌	법인은 벌금형	CEO **형사처벌가능**	법인은 벌금형

기업은 어떻게 대처해야 하는가?

1. 파기절차/방법을 포함한 〈개인정보취급방침〉 공개
2. 개인정보 미파기 **6대 위험ZONE** 점검



〈점검→파기〉 주기적 검출→ 복구재생 불가한 방법으로 파기→ 불필요한 개인정보 복제 차단

CPO에게 보고 → CEO에게 보고

〈미점검 → 미파기〉 관련 상세규정 보기

<table>
<tr><th>조항</th><th>개정여부</th><th>내용</th></tr>
<tr><td>27조</td><td>신설</td><td>④ CPO는 이 법 및 다른 관계 법령 위반사실을 알게 된 경우,
즉시 개선조치를 하고 필요시 사업주 or 대표자에게 개선조치 보고</td></tr>
<tr><td>27조
의2</td><td>기존</td><td>② 개인정보 처리방침에는 다음 각 호의 사항이 모두 포함되어야 한다.
3. 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법</td></tr>
<tr><td>29조</td><td>기존</td><td>① 개인정보 보유,이용기간이 끝났거나 수집이용목적이 달성되면 복구/재생할 수 없도록 파기해야 한다
② 정보통신서비스 제공자등은 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다. (위반시 과태료 3천만원)
③ 정보통신서비스 제공자등은 제2항의 기간 만료 30일 전까지 개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목 등 대통령령으로 정하는 사항을 전자우편 등 대통령령으로 정하는 방법으로 이용자에게 알려야 한다.</td></tr>
<tr><td rowspan="2">32조
의3</td><td rowspan="2">신설</td><td>① 주민번호, 계좌정보, 카드정보 등 개인정보가 정보통신망을 통하여 공중에 노출되지 않도록 하여야 한다.</td></tr>
<tr><td>② 방통위 or KISA 요청시, ①의 노출된 개인정보에 대한 삭제 · 차단 등 필요한 조치를 취하여야 한다.
(위반시 과태료 3천만원)</td></tr>
<tr><td rowspan="3">64조</td><td>기존</td><td>① 다음 경우 미래부 or 방통위는 관계 물품 · 서류 등을 제출 요구할 수 있다
1. 법위반사항을 발견 or 혐의를 알게 된 경우 2. 이 법의 위반에 대한 신고를 받거나 민원이 접수된 경우
2의2. 이용자 정보의 안전성과 신뢰성 확보를 현저히 해치는 사건 · 사고 등이 발생하였거나 발생할 가능성이 있는 경우</td></tr>
<tr><td>기존</td><td>② 방통위는 (이 법을 위반, 영리목적 광고성 정보를 전송한 자에게 조치를 하기 위하여)
해당 광고성 정보 전송자의 성명 · 주소 · 주민등록번호 · 이용기간 등에 대한 자료의 열람이나 제출을 요청할 수 있다.</td></tr>
<tr><td>개정</td><td>③ 미래부 or 방통위는 〈정보통신서비스제공자〉가 ① 및 ②에 따른 자료를 제출하지 아니하거나
이 법을 위반한 사실이 있다고 인정되면 소속공무원에게 정보통신서비스 제공자등, 해당 법 위반 사실과 관련한 관계인의 사업장에 출입하여 업무상황, 장부 or 서류 등을 검사하도록 할 수 있다.</td></tr>
<tr><td>69조
의2</td><td>신설</td><td>② 방통위는 이 법을 위반한 〈정보통신서비스제공자〉에게 책임있는 자(대표자 및 책임있는 임원을 포함한다)를 징계할 것을 권고할 수 있다. 이 경우 이를 존중하여야 하며 그 결과를 방통위에 통보하여야 한다.</td></tr>
<tr><td>75조
의2</td><td>신설</td><td>
<table>
<tr><th>조항</th><th colspan="2">내용</th><th>처벌</th></tr>
<tr><td rowspan="8">71조</td><td rowspan="4">이용자의 동의를 받지 아니하고</td><td>① 개인정보를 수집한 자</td><td rowspan="8">5년이하 징역
or
5천만원 이하 벌금</td></tr>
<tr><td>② 개인의 권리/이익, 사생활을 침해할 우려가 있는 개인정보를 수집한 자</td></tr>
<tr><td>③ 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 or 부정한 목적으로 개인정보를 제공받은 자</td></tr>
<tr><td>④ 개인정보 취급위탁을 한 자</td></tr>
<tr><td colspan="2">⑤ 이용자의 개인정보를 훼손/침해 or 누설한 자</td></tr>
<tr><td colspan="2">⑥ 개인정보가 누설된 사정을 알면서도 영리 or 부정한 목적으로 개인정보를 제공받은 자</td></tr>
<tr><td colspan="2">⑦ (이용자가 정정요구한 경우에도) 필요한 조치 없이 개인정보를 제공하거나 이용한 자</td></tr>
<tr><td colspan="2">⑧ 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 자</td></tr>
<tr><td>72조</td><td colspan="2">② (정보통신망을 통하여 속이는 행위로) 다른 사람의 개인정보를 수집한 자 (49조 ①)</td><td>3년이하 징역
or
3천만원 이하 벌금</td></tr>
<tr><td rowspan="3">73조</td><td colspan="2">① (망법고시 〈개인정보의 기술적 관리적 보호조치기준〉 위반으로) 기술적 · 관리적 조치를 하지 아니하여 이용자의 개인정보를 분실/도난/누출/변조 or 훼손한 자</td><td rowspan="3">2년이하 징역
or
2천만원 이하 벌금</td></tr>
<tr><td colspan="2">①의2. (보유이용기간이 종료된 경우 복구재생되지않는 방법으로) 개인정보를 파기하지 아니한 자</td></tr>
<tr><td colspan="2">⑦ (정보통신망을 통하여 속이는 행위로) 개인정보의 제공을 유인한 자</td></tr>
</table>

+ 몰수, 추징
해당 위반행위와 관련하여 취득한 금품이나 그 밖의 이익은 몰수할 수 있으며, 불가능할 경우 그 가액을 추징 할 수 있다.
</td></tr>
</table>

발송일
2016. 03

3.22일 공포, 9.23일 시행

2016년 개정, 정보통신망법 변화 ③ 이외 규정

<table>
<tr><th>조항</th><th>개정여부</th><th>내용</th></tr>
<tr><td rowspan="2">22조의2</td><td>신설</td><td>① 〈이용자의 이동통신단말장치 기능 및 저장된 정보〉에 대한 접근권한이 필요한 경우 동의를 받아야한다
<table>
<tr><td>권한종류</td><td>1. 〈반드시 필요한 접근권한〉</td><td>2. 〈반드시 필요하지 않은 접근권한〉인 경우</td></tr>
<tr><td>동의항목</td><td>가. 정보 및 기능의 항목
나. 접근권한이 필요한 이유</td><td>가. 정보 및 기능의 항목 나. 접근권한이 필요한 이유
다. 동의하지 아니할 수 있다는 사실</td></tr>
</table></td></tr>
<tr><td>신설</td><td>② 〈반드시 필요하지 않은 접근권한〉 설정에 동의하지 않았다는 이유로, 서비스 제공을 거부할 수 없다
<table>
<tr><td rowspan="2">③</td><td>아래 업체 대상으로</td><td>다음 경우에</td><td>〈이용자 정보보호조치〉 의무화</td><td>위반시 처벌</td></tr>
<tr><td>이동통신 단말 장치의</td><td>1. 제조업자,
2. SW제작공급자
3. OS 공급자</td><td>〈정보통신서비스제공자〉가 〈이동통신단말장치〉기능 및 저장된 정보에 접근할 경우</td><td>접근권한에 대한 이용자의 동의 및 철회방법을 마련하는 등〈이용자정보 보호조치〉를 해야한다 (대통령령에서 구체화)</td><td>과태료 3천만원</td></tr>
</table></td></tr>
<tr><td>24조의2</td><td>개정</td><td>
<table>
<tr><td rowspan="2">· 용어변경(취급→처리)
· 처리의 개념확대</td><td colspan="2">기존 취급의 개념 → 현재 처리의 개념</td></tr>
<tr><td>수집, 보관, 처리, 이용, 제공, 관리, 파기 등</td><td>수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위</td></tr>
</table></td></tr>
<tr><td rowspan="4">25조</td><td>기존</td><td>① 개인정보 처리위탁시 이용자에게 1. 처리위탁을 받는 자 2. 처리위탁업무내용을 알리고 동의를 받아야한다</td></tr>
<tr><td>개정</td><td>④ 수탁자가 이 장의 규정을 위반하지 아니하도록 관리 · 감독 및 교육하여야 한다.</td></tr>
<tr><td>신설</td><td>⑥ 수탁자에게 개인정보 처리위탁시 문서에 의하여야 한다. 위반시 과태료 1천만원 이하</td></tr>
<tr><td>신설</td><td>⑦ 수탁자가 제3자에게 재위탁할 경우에는 〈정보통신서비스제공자〉의 동의를 받아야만 한다 〈신설〉 위반시 과태료 2천만원 이하</td></tr>
<tr><td>44조의7</td><td>신설</td><td>① 정보통신망에서 유통되어서는 안되는 불법정보
6의2호. 이 법 or 개인정보보호에 관한 법령을 위반, 개인정보를 거래하는 내용의 정보</td></tr>
<tr><td rowspan="4">49조의2</td><td>기존</td><td>① 누구든지 정보통신망을 통하여 속이는 행위로 다른 사람의 정보를 수집하거나 다른 사람이 정보를 제공하도록 유인하여서는 아니 된다.</td></tr>
<tr><td>개정</td><td>② 〈정보통신서비스 제공자〉는 ①의 위반사실을 발견하면 즉시 미래부 or 방통위 or KISA에 신고하여야 한다.</td></tr>
<tr><td>신설</td><td>③ 미래부 or 방통위 or KISA는 ②의 신고를 받거나 ①의 위반사실을 알게 되면 다음 조치를 하여야 한다.
<table>
<tr><td>1</td><td>기존</td><td>위반 사실에 관한 정보의 수집 · 전파</td></tr>
<tr><td>2</td><td>기존</td><td>유사 피해에 대한 예보 · 경보</td></tr>
<tr><td>3</td><td>개정</td><td>〈정보통신서비스 제공자〉에게 접속경로의 차단 or
이용자에게 ①의 위반행위에 노출되었다는 사실을 알리도록
요청 등 피해예방 및 피해 확산을 방지하기 위한 긴급조치</td></tr>
</table>
〈신설 부칙3조〉
(위반행위에 노출된 사실 안내에 관한 경과조치)
〈정보통신서비스제공자〉는 법이 공포된 후 6개월 이내에 이용자에게 안내메시지를 보낼 수 있는 설비를 구축하여야 한다.</td></tr>
<tr><td>신설</td><td>④ 미래부 or 방통위는 ③항 3호의 조치를 취하기 위하여 〈정보통신서비스 제공자〉에게 〈정보통신서비스 제공자〉 간 정보통신망을 통하여 속이는 행위에 대한 정보 공유 등 필요한 조치를 취하도록 명할 수 있다</td></tr>
<tr><td>63조 ②항</td><td>신설</td><td>
<table>
<tr><th>〈이용자동의〉를 받아야하는 국외이전</th><th>국외 이전시 〈이용자동의〉를 생략할 수 있는 경우</th><th>처벌</th></tr>
<tr><td>국외에 제공(조회 포함)</td><td>생략할 수 없음</td><td rowspan="2">과태료 2천만원 이하</td></tr>
<tr><td>국외에 처리위탁, 보관</td><td>계약이행과 이용자 편의증진에 필요한 경우로서 ③항 각 호의 사항 모두를 27조의2 ①에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우</td></tr>
</table>
63조 ③ (국외 이전 개인정보의 보호)
정보통신서비스 제공자등은 ②에 따른 동의를 받으려면 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다
1. 이전되는 개인정보 항목 2. 개인정보가 이전되는 국가, 이전일시 및 이전방법
3. 개인정보를 이전받는 자의 성명(법인 경우명칭 및 정보관리책임자의 연락처)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유 · 이용 기간

27조의2 (개인정보 취급방침의 공개) ①
정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 경우에는 개인정보 취급방침을 정하여 이용자가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.</td></tr>
<tr><td>70조의2</td><td>신설</td><td>악성프로그램을 전달 or 유포하는 자는 7년 이하의 징역 or 7천만원 이하의 벌금에 처한다.</td></tr>
<tr><td>71조</td><td>신설</td><td>① 9. 정보통신망에 침입한 자 – 5년 이하의 징역 or 5천만원 이하의 벌금에 처한다
② 정보통신망 침입미수범도 처벌</td></tr>
</table>

03

PIMS인증

(적용대상 : 공공기관 · 대기업 · 중소기업 · 소상공인)

발송일
2015. 12

2016년 1월1일부터

기존 PIPL인증(평가항목 65개) 과 기존 PIMS인증(평가항목 124개)을 PIMS인증(평가항목 86개)으로 통합 ①

보안분야인증 어떻게 변화하고 있나?

인증 명칭	PIMS인증	PIPL인증		
시행 시기	2010년 11월	2013년 11월		
인증 대상	영리목적의 정보통신서비스기업	공공/ 대기업	중소 기업	소상 공인
평가 항목	124개	65개	52개	33개
근거 법률	정보통신망법	개인정보보호법		
수행 기관	방송통신위원회 & KISA	행정자치부 & NIA		

이전 Report 보기 이전 Report 보기

=

[확정] 개인정보보호인증은 〈PIMS인증〉으로 통합

[추진중] 일정규모이상 조직대상 〈PIMS인증〉의무화

발의법안 바로가기

PIMS(개인정보관리체계) 인증
2016년1월
공공기관 86개 대기업 84개 중소기업 72개 소상공인 47개
개인정보보호법 + 정보통신망법
행정자치부,방송통신위원회 & KISA

[대상]
기간통신사업자, 집적정보통신사업자
매출 100억 or 일평균이용자 100만명 이상
정보통신사업자대상으로

2013년 2월
〈ISMS(정보보호관리체계)인증〉의무화

이전 Report 보기

[대상]
ISMS인증을 3년 유지한 사업자에게
정보보호관리
〈우수〉〈최우수〉 등급부여

이전 Report 보기

[확정] 정보보호 인증제도 〈ISMS인증〉강화

2015년 미래부 발표문 바로가기

〈ISMS인증〉 의무화대상을
일정규모이상 조직 대상으로 (정보통신 외에)
의료, 교육, 에너지 분야로 확대

〈ISMS인증〉 미획득시 과태료 상향
(1,000만원 → 3,000만원)

〈통합 PIMS인증〉 중 기술적 보호조치 항목 1/3

1. 관리체계 (7) 정책(3) 조직(3) 경영진책임(1)	2. 식별 및 위험관리 (5) 식별(2) 위험관리(3)	3. 보호체계 점검 (4) 체계검토(2) 개선활동(1) 내부공유 및 교육(1)	4. 생명주기별 보호조치 (14) 수집(6) 제공(4) 보유(2) 파기(2)	5. 정보주체 권리보장 (3)
6. 관리적 보호조치 (12) 교육훈련(1) 취급자(3) 위탁(3) 침해사고(5)	**7. 기술적 보호조치(32)** 접근권한(7) 접속기록(2) 운영보안(16) 암호화통제(2) 개발보안(5)	8. 물리적보호조치(9) 영상정보처리기기관리(2) 물리적보안(4) 매체및출력물관리(3)		

항목	기준	기존 인증기준 내 동일항목 존재여부		상세내용	적용대상				솔루션
		기존PIMS	PIPL		공공	대기업	중소기업	소상공인	
7.1 접근권한관리	7.1.1 접근통제 정책수립	O (나7.1.1)	O (8.3.5)	〈취급자〉대상 〈접근통제 정책〉 수립 (접근통제 영역 및 범위, 규칙, 방법 등 포함)	O	O			〈개인정보처리시스템〉 접근통제 및 접속기록 관리 [DB] DB-i [WAS] WAS-i [SAP] App-i
	7.1.2 〈취급자〉등록	O (나7.1.2)	O (8.1.1)	개인정보,〈개인정보처리시스템〉대상 접근통제를 위한 공식적 〈취급자〉 등록 ,해지 절차 마련, 접근권한 최소화	O	O	O	O	
	7.1.3 〈취급자〉 권한관리	O (나7.1.3)	O (8.1.2)	〈개인정보처리시스템〉접근권한은 최소한의 업무수행자에게만 부여, 권한 생성, 변경, 말소 내역 보관 / 관리	O	O	O	O	
	7.1.4 특수권한관리	O (나7.1.8)	O (8.1.2)	개인정보, 〈개인정보처리시스템〉대상 특수목적 계정, 권한을 식별, 별도 통제	O	O	O	O	
	7.1.5 〈취급자〉 접근권한검토	O (나7.1.4)	O (8.1.3)	개인정보, 〈개인정보처리시스템〉 을 사용하는 〈취급자〉접근권한 현황을 정기적으로 점검	O	O	O		
	7.1.6 〈취급자〉 인증 식별	O (나7.1.5)	X	〈개인정보처리시스템〉접근을 〈안전한 인증절차〉에 따라 통제: 〈취급자〉인증, 로그인횟수제한, 세션타임아웃, 불법 로그인 시도 경고 등 필요시 강화된 인증방식 적용	O	O	O	O	
	7.1.7 패스워드 관리	O (나7.1.7)	O (8.2.1)	〈패스워드 관리절차〉 수립·관리 (패스워드 복잡도, 초기 패스워드 변경, 변경주기 등)	O	O	O	O	
7.2 접속기록관리	7.2.1 〈개인정보처리시스템〉 접속기록관리	O (나7.6.2)	O (8.2.1)	〈개인정보처리시스템〉(응용프로그램, DB 등) 접속기록 (식별자, 접속일시, 열람 · 수정 · 삭제 · 출력 등의 작업내역) 보관, 관리 접속기록 정확성 보장을 위해 장비,시스템 표준시각 동기화	O	O	O	O	
	7.2.2 접속기록 모니터링 /점검	O (나7.6.3 나7.6.4)	O (8.2.1)	접속기록 위·변조방지를 위하여 보안통제 적용 (접근권한통제, 별도의 물리적 저장장치 보관 등) 〈지침, 절차〉 수립 → 개인정보처리활동 모니터링, 정기점검 →사후조치	O	O	O		

〈통합 PIMS인증〉 중 기술적 보호조치 항목 2/3

항목	기준	기존 인증기준 내 동일항목 존재여부		상세내용	적용대상				솔루션
		기존PIMS	PIPL		공공	대기업	중소기업	소상공인	
7.3 운영보안	7.3.1 운영절차수립	O (나7.3.1)	X	〈개인정보처리시스템〉 문제 발생시 운영절차 수립 (재동작 / 복구, 오류 / 예외사항 처리 등)	O	O			
	7.3.2 직무분리	O (나7.3.2)	X	고의 or 부주의로 인한 〈개인정보처리시스템〉 오남용예방을 위해 〈직무분리기준〉수립/적용 어려운 경우 별도의 〈관리감독/ 보완통제 대책〉 마련	O	O			
	7.3.3 악성코드통제	O (나7.3.8)	O (8.3.2)	바이러스, 웜, 트로이목마 등의 〈악성코드 예방, 탐지, 대응 등의 보호대책〉 수립	O	O	O	O	[세이프브라우징] WebKeeper Virus, APT 솔루션
	7.3.4 비인가 접근 모니터링/ 취약점 점검	O (나7.3.11)	O (8.3.3)	· 〈개인정보처리시스템〉비인가접근 예방을 위한 모니터링 · (알려진) 취약점노출여부 확인을 위해 정기적 기술적취약점 점검→조치	O	O	O		개인정보처리시스템 접근통제 [DB] DB-i [WAS] WAS-i [SAP] App-i 취약점 점검 스캐너
	7.3.5 개인정보 표시제한	O (나7.8.1)	O (8.3.4)	조회, 출력시 마스킹 기술 등을 통해 개인정보표시 제한	O	O	O		어플리케이션 개발시 개인정보마스킹 DB-i
	7.3.6 접근통제/ 보안시스템 설치·운용	X	O (8.3.5)	· 불법접근,침해사고 방지를 위해 침입차단, 탐지기능을 포함한 시스템 설치 · 운용 · 보안시스템 유형별로 〈운영절차〉수립 (관리자 지정, 정책 업데이트, 룰셋변경, 이벤트 모니터링 등) 정책적용 현황 관리	O	O	O		개인정보처리시스템 접근통제 [DB] DB-i [WAS] WAS-i [SAP] App-i 일반방화벽, IPS
	7.3.7 네트워크 접근	O (나7.1.9)	O (8.3.6)	· 비인가접근 통제를 위해 〈관리절차〉 수립 (네트워크 접근통제리스트, 네트워크 식별자 등을 관리) · 서비스, 사용자그룹, 개인정보자산중요도, 법적요구사항에 따라 내 · 외부 네트워크 분리	O	O	O	O	[Network DLP] Mail-i Mail-i For WebDLP 망분리솔루션
	7.3.8 서버 접근	O (나7.1.10)	X	서버별로 접근허용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 적용	O	O	O	O	서버접근통제
	7.3.9 응용프로그램 접근	O (나7.1.11)	X	업무 or 직무에 따라 응용프로그램 접근권한을 제한, 불필요한 개인정보노출 최소화	O	O	O	O	[WAS] WAS-i [SAP] App-i

〈통합 PIMS인증〉 중 기술적 보호조치 항목 3/3

항목	기준	기존 인증기준 내 동일항목 존재여부		상세내용	적용대상				솔루션
		기존PIMS	PIPL		공공	대기업	중소기업	소상공인	
	7.3.10 데이터베이스 접근	O (나 7.1.12)	X	· DB접근을 허용하는 응용프로그램 &사용자대상 직무 정의, 응용프로그램별, 직무별 〈접근통제 정책〉 수립 · DB대상 사용자 접근내역 기록 및 접근타당성정기검토 수행	O	O	O	O	개인정보처리시스템 접근통제 [DB] DB-i [WAS] WAS-i [SAP] App-i Endpoint DLP Privacy-i
	7.3.11 원격 운영 관리	O (나7.3.4)	O (8.3.7)	· 〈개인정보처리시스템〉은 내부네트워크, 특정단말로만 접근 · 원격지에서 인터넷 등 외부네트워크 접근은 원칙적금지, · 허용시 〈보호대책〉 수립 (책임자 승인, 단말/사용자 인증, 구간암호화, 단말기보안 – 백신, 패치 등)	O	O	O		
	7.3.12 공개서버 보안	O (나 7.3.7)	X	· 웹사이트에 정보공개시 정보수집, 저장, 공개에 따른 〈허가, 게시절차〉 수립, · 공개서버에 대한 〈물리적, 기술적 보호대책〉 수립	O	O	O	O	Server-i
7.3 운영보안	7.3.13 인터넷접속 통제	O (나7.1.14)	X	〈개인정보처리시스템〉에 접근가능한 〈취급자〉PC는 인터넷접속 or 서비스(P2P, 웹메일, 웹하드, 메신저 등) 제한/통제, 필요시 인터넷 접속내역 모니터링	O	O	O		[세이프 브라우징] WebKeeper [Network DLP] Mail-i
	7.3.14 모바일기기 관리	O (나7.1.13)	X	업무목적으로 모바일기기를 내 · 외부 네트워크에 연결시 〈접근통제대책〉 수립 (사용자인증/ 승인, 접근 범위, 기기 보안설정, 송수신 데이터 암호화, 오남용 모니터링 등)	O	O	O		Mobile-i
	7.3.15 백업관리	O (나7.3.10)	X	데이터무결성, 〈개인정보처리시스템〉가용성 유지를 위해 〈백업 대상/주기/방법 절차〉 수립 →주기적 백업 / 관리	O	O			
	7.3.16 패치관리	O (나7.3.9)	X	SW, 운영체계, 보안시스템 등의 시스템에 미치는 영향분석 → 주기적 최신패치 적용	O	O	O	O	
7.4 암호화통제	7.4.1 암호화정책 수립	O (나7.2.1)	O (8.4.1)	· 법적요구사항을 반드시 반영한 〈암호화 정책〉 수립 · 암호화대상, 강도(복잡도), 키관리(암호키 생성, 이용, 보관, 배포, 파기, 복구방안), 저장/전송 시 암호화 적용 등	O	O	O		[서버] Server-i [PC] Privacy-i DB 암호화솔루션
	7.4.2 암호화 적용	X	O (8.4.2)	〈암호화정책〉에 따라 저장/전송시 & 원격접속시 암호화	O	O	O	O	

발송일
2015. 12

2016년 1월1일부터

기존 PIPL인증(평가항목 65개) 과 기존 PIMS인증(평가항목 124개)을 PIMS인증(평가항목 86개)으로 통합 ②

보안분야인증 어떻게 변화하고 있나?

인증 명칭	PIMS인증	PIPL인증		
시행 시기	2010년 11월	2013년 11월		
인증 대상	영리목적의 정보통신서비스기업	공공/ 대기업	중소 기업	소상 공인
평가 항목	124개	65개	52개	33개
근거 법률	정보통신망법	개인정보보호법		
수행 기관	방송통신위원회 & KISA	행정자치부 & NIA		

이전 Report 보기 이전 Report 보기

=

[확정] 개인정보보호인증은 〈PIMS인증〉으로 통합

[추진중] 일정규모이상 조직대상 〈PIMS인증〉의무화

발의법안 바로가기

PIMS(개인정보관리체계) 인증
2016년1월
공공기관 86개 대기업 84개 중소기업 72개 소상공인 47개
개인정보보호법 + 정보통신망법
행정자치부,방송통신위원회 & KISA

[대상]
기간통신사업자, 집적정보통신사업자
매출 100억 or 일평균이용자 100만명 이상
정보통신사업자대상으로

2013년 2월
〈ISMS(정보보호관리체계)인증〉의무화

이전 Report 보기

[대상]
ISMS인증을 3년 유지한 사업자에게
정보보호관리 〈우수〉 〈최우수〉 등급부여

이전 Report 보기

[확정] 정보보호 인증제도 〈ISMS인증〉강화

2015년 미래부 발표문 바로가기

〈ISMS인증〉 의무화대상을
일정규모이상 조직 대상으로 (정보통신 외에)
의료, 교육, 에너지 분야로 확대

〈ISMS인증〉 미획득시 과태료 상향
(1,000만원 → 3,000만원)

〈통합 PIMS인증〉 중 기술적 보호조치 외 나머지 항목 1/9

1. 관리체계 (7) 정책(3) 조직(3) 경영진책임(1)	2. 식별 및 위험관리 (5) 식별(2) 위험관리(3)	3. 보호체계 점검 (4) 체계검토(2) 개선활동(1) 내부공유 및 교육(1)	4. 생명주기별 보호조치 (14) 수집(6) 제공(4) 보유(2) 파기(2)	5. 정보주체 권리보장 (3)
6. 관리적 보호조치 (12) 교육훈련(1) 취급자(3) 위탁(3) 침해사고(5)	7. 기술적 보호조치(32) 접근권한(7) 접속기록(2) 운영보안(16) 암호화통제(2) 개발보안(5)		8. 물리적보호조치(9) 영상정보처리기기관리(2) 물리적보안(4) 매체및출력물관리(3)	

1. 관리체계 (7개항목)

항목	기준	기존 인증기준 내 동일항목 존재여부		상세내용	적용대상			
		기존PIMS	PIPL		공공	대기업	중소기업	소상공인
1.1 정책 범위	1.1.1 정책수립	O (나1.1.2)	O (1.1.1 4.2.1)	조직방침 / 방향제시를 위해 〈개인정보보호정책,시행문서〉 수립 →〈CPO〉승인 → 임직원 / 관련자에게 공표	O	O	O	O
	1.1.2 정책유지 관리	O (나1.3.1)	X	〈개인정보보호정책,시행문서〉는 법·규제를 준수, 일관성 유지 신규위협·취약성 & 시스템환경변화 등을 정기적검토	O	O	O	
	1.1.3 범위설정	O (가1.2)	O (1.1.2)	〈개인정보보호 관리체계〉 범위설정 (중요업무, 서비스, 조직, 자산 등을 포함) → 범위 내 모든 자산을 식별,문서화	O	O	O	
	[요구사항] DB, 서버, PC 내 개인정보검출 〈개인정보보호관리체계〉 내 모든 개인정보자산을 식별하기 위하여 조직내 DB, 서버, PC 내 개인정보를 검출 →불필요한 개인정보 파기 →문서화			[필요솔루션] 개인정보보유현황분석&파기 DB, 서버 내 개인정보 Server-i PC, 모바일 내 개인정보 Privacy-i				
1.2 조직	1.2.1 〈CPO〉지정	O (나 2.2.1)	O (7.1.1)	〈CEO〉는 지속적 〈관리체계〉 운영을 위하여 〈CPO〉 지정	O	O	O	O
	1.2.2 조직구성	O (가2.2)	X	조직규모, 업무중요도분석을 통해 실무조직, 개인정보보호 관련사항 검토 / 의사결정기구 구성	O	O	O	
	1.2.3 역할 / 책임	O (나2.2.1)	O (1.2.1)	〈CPO〉, 개인정보취급부서책임자& 담당자 역할과 책임 정의, 평가체계 마련	O	O	O	
1.3 경영 진책 임	1.3.1 경영진의 참여	O (가2.1)	O (1.3.1)	〈관리체계〉수립, 운영 등 개인정보보호 활동 전반에 경영진참여를 위하여 〈보고/의사결정 체계〉 수립	O	O		

개인정보보호관리책임자 〈CPO〉, 개인정보보호관리체계 〈관리체계〉, 개인정보흐름도 〈흐름도〉

〈통합 PIMS인증〉 중 기술적 보호조치 외 나머지 항목 2/9

2. 식별 및 위험관리 (5개항목)

항목	기준	기존 인증기준 내 동일항목 존재여부		상세내용	적용대상			
		기존PIMS	PIPL		공공	대기업	중소기업	소상공인
2.1 개인정보 식별	2.1.1 개인정보 식별	O (나 3.1.1 나 3.2.1)	O (2.2.1)	개인정보&자산 (개인정보처리시스템, 개인정보DB, 개인정보파일 등) 식별 → 자산별로 업무영향, 법적 준수사항 등을 고려, 중요도 결정 → 소유자/관리자/〈취급자〉 확인→ 책임소재정의 → 식별된 개인정보와 관리자산에 보안등급 부여 → 취급절차 정의·이행	O	O	O	O
	[요구사항] DB, 서버, PC 내 개인정보검출 개인정보&자산 식별을 위하여 조직내 DB, 서버, PC내 개인정보를 검출 →불필요한 개인정보 파기			[필요솔루션] 개인정보보유현황분석&파기 DB, 서버 내 개인정보 Server-i PC, 모바일 내 개인정보 Privacy-i				
	2.1.2 개인정보 흐름 파악	O (가1.3)	O (2.3.2)	개인정보흐름 파악→〈흐름도〉 작성 (흐름도는 주기적으로 검토, 최신성 유지)	O	O	O	X
	[요구사항] DB, 서버, PC, 네트워크, 출력, 모바일, USB 간 개인정보흐름 기록 및 파악			[필요솔루션] 개인정보처리시스템접속기록관리솔루션 DB-i, WAS-i Network DLP (네트워크를 통한 외부전송기록) Mail-i EndPoint DLP (출력물, 매체복사를 통한 외부전송기록) Privacy-i				
	2.2.1 위험관리 방법 계획 수립	O (가3.1)	O (2.3.1)	〈CEO〉는 지속적 〈관리체계〉 운영을 위하여 〈CPO〉 지정	O	O	O	
2.2 위험관리	2.2.2 위험식별 평가	O (가3.2)	O (2.3.2)	〈위험관리계획〉에 따라 〈위험식별/평가〉를 연1회 이상 수행, → 결과에 따라 〈수용가능한 위험수준〉 선정, 관리	O	O	O	
	[요구사항] 〈위험식별/평가〉의 출발점은 정확한〈개인정보자산식별〉임			[필요솔루션] 개인정보보유현황분석&파기 DB, 서버 내 개인정보 Server-i PC, 모바일 내 개인정보 Privacy-i				
	2.2.3 이행계획 수립 보호대책 구현	O (가3.3)	O (2.3.4)	위험을 수용가능수준으로 감소시키기 위해 〈보호대책〉구현 →〈이행계획〉 수립 (우선순위, 일정, 담당부서, 담당자 , 예산 등을 포함) →경영진승인→ 보호대책 구현	O	O	O	

〈통합 PIMS인증〉 중 기술적 보호조치 외 나머지 항목 3/9

3. 개인정보 보호체계 점검(4개항목)

항목	기준	기존 인증기준 내 동일항목 존재여부		상세내용	적용대상			
		기존PIMS	PIPL		공공	대기업	중소기업	소상공인
3.1 보호체계 검토	3.1.1 법적사항 준수검토	O (가5.1)	O (2.3.2)	법적요구사항을 파악, 최신성 유지, 준수여부 지속적 검토	O	O	O	O
	3.2.1 내부감사	O (가5.3)	O (3.1.1 3.1.2)	내부감사 연 1회 이상 수행, 독립적&전문적 감사인력 구성 감사기준, 범위, 주기, 방법 결정 → 문제점 보완조치 완료 → 경영진 / 책임자보고	O	O	O	
3.2 교정 개선	3.2.1 개선활동	O (가5.2)	O (2.1.1 4.1.1)	개인정보 보호 활동을 문서화,운영현황 지속적 점검개선	O	O	O	
	[요구사항] · 내부감사시 사내 보유한 개인정보식별→ 파기 · 중요개인정보의 외부로의 흐름파악			[필요솔루션] 개인정보보유현황분석&파기 DB, 서버 내 개인정보 Server-i PC, 모바일 내 개인정보 Privacy-i				
3.3 내부공유 /교육	3.3.1 내부공유 /교육	O (가2.2)	X	〈개인정보보호대책〉을 운영 or 시행할 부서, 담당자에게 내용공유 및 교육	O	O	O	O

〈통합 PIMS인증〉 중 기술적 보호조치 외 나머지 항목 4/9

4. 생명주기별보호조치 (14개항목)

항목	기준	기존 인증기준 내 동일항목 존재여부		상세내용	적용대상			
		기존PIMS	PIPL		공공	대기업	중소기업	소상공인
4.1 수집시 보호조치	4.1.1 수집제한	O (다1.1.1)	O (5.1.1)	서비스제공을 위한 최소한 정보를 수집, 수집시 필수와 선택사항으로 구분, 선택사항정보 미제공을 이유로 서비스제공을 거부할수없음	O	O	O	O
	4.1.2 동의	O (다1.2.1)	O (5.1.2)	법령에 규정이 있는 경우를 제외하고는 〈정보주체〉의 동의를 얻은 후에 수집	O	O	O	O
	4.1.3 민감정보/고유식별정보 수집제한	O (다1.1.2)	O (5.1.4)	〈고유식별정보〉와 〈민감정보〉는 〈정보주체〉의 동의 or 법령에 따라 허용된 경우를 제외하고는 수집할 수 없음	O	O	O	O
	4.1.4 간접수집 보호조치	O (다1.1.3)	O (5.1.5)	〈간접수집개인정보〉(시스템에 의한 수집 or 처리 중 생성) 에 대하여 〈보호대책〉수립 · 이행	O	O	O	O
	4.1.5 주민번호 수집이용 제한	O (다1.1.4)	O (5.1.4)	법령에서 허용한 경우를 제외하고 주민번호 수집 이용금지	O	O	O	O
	4.1.6 주민번호 대체수단	O (다1.1.5)	O (5.1.6)	법령에서 허용한 경우에도 〈주민번호 대체수단〉(공인인증서, 아이핀 등) 제공	O	O	O	O

[요구사항] 수집을 제대로 하는지 어떻게 확인할 것인가

4.1.1 최소한의 정보를 수집하였는지?
4.1.2 법령상 수집할 수 없는 정보를 수집하였는지?
4.1.3 〈고유식별정보〉와 〈민감정보〉를 수집하였는지?
4.1.4 〈간접수집개인정보〉가 얼마나 생성되었는지?
4.1.5 〈주민번호〉를 수집이용중인지?
4.1.6 〈주민번호대체수단〉을 적용해야 할 주민번호가 있는지 ?

알기 위하여 DB, 서버, PC에 저장된개인정보 검출,
특히 최근에 생성된 DB테이블과 파일을 중점조사

[필요솔루션]
개인정보보유현황분석&파기

DB, 서버 내 개인정보 Server-i
PC, 모바일 내 개인정보 Privacy-i

〈통합 PIMS인증〉 중 기술적 보호조치 외 나머지 항목 5/9

항목	기준	기존 인증기준 내 동일항목 존재여부		상세내용	적용대상			
		기존PIMS	PIPL		공공	대기업	중소기업	소상공인
4.2 이용/제공시 보호조치	4.2.1 제3자 제공	O (다2.4.1 다2.4.3)	O (5.2.1)	〈정보주체〉에게 제공받는자, 제공목적등을 고지 → 동의획득후 제공, 제3자에게 접근허용시 〈보호절차〉에 따라 통제	O	O	O	O
	4.2.2 제공받은 개인정보 관리	O (다2.4.2)	O (5.2.2)	목적외용도로 이용금지, 제3자에게 제공불가, 안전하게 관리	O	O	O	O
	4.2.3 목적외 이용/제공	O (다2.4.2)	O (5.2.2)	〈정보주체〉에게 고지,동의받은 범위 내에서 이용, 동의범위를 벗어날 경우 〈정보주체〉로부터 추가동의 획득, 보호조치	O	O	O	O
	4.2.4 개인정보 이전	O (다2.5.1 다2.5.2)	O (5.2.3)	영업양도, 합병 등으로 개인정보 이전시 〈보호대책〉 수립·이행 해외이전시 〈정보주체〉동의획득 → 〈보호대책〉 수립·이행	O	O	O	O
	[요구사항] · 외부에서 접근가능한 웹어플리케이션이 DB와 연계연동하여 누구의 개인정보에 접근하는지, 과다하게 가져가는지, 제3자가 가져가는지 확인한다 · 네트워크, 출력물, USB로 정보 제공시 누구의 개인정보에 접근하는지, 과다하게 가져가는지, 제3자가 가져가는지 확인한다 · 3자제공시마다 결재 등의 보고절차를 거쳐서 목적에 부합하는 제공인지 확인한다.			[필요솔루션] 웹어플리케이션을 통한 개인정보 3자제공시 기록 WAS-i 네트워크를 통한 개인정보 3자제공시 기록, 차단, 결재 Mail-i 출력물, USB를 통한 개인정보 3자제공시 기록, 차단, 결재 Privacy-i				
4.3 보유시 보호조치	4.3.1 품질 보장	O (다3.1.1)	O (5.3.1)	수집된 개인정보는 안전하게 저장 , 관리 정확성, 안전성, 최신성 유지	O	O	O	O
	4.3.2 파일관리	X	O (5.3.2)	개인정보파일을 운용하는 공공기관은 운영 현황을 행정자치부에 등록, 변경시 고지	O	O	O	O
	[요구사항] DB, 서버, PC내 개인정보검출 조직내 DB, 서버, PC 내 개인정보를 검출 →불필요한 개인정보 파기 →행정자치부에 등록			[필요솔루션] 개인정보 보유현황분석&파기 DB, 서버 내 개인정보 Server-i PC, 모바일 내 개인정보 Privacy-i				

〈통합 PIMS인증〉 중 기술적 보호조치 외 나머지 항목 6/9

4. 생명주기별보호조치 (14개항목) 앞장에서 계속

항목	기준	기존 인증기준 내 동일항목 존재여부		상세내용	적용대상			
		기존PIMS	PIPL		공공	대기업	중소기업	소상공인
4.4 파기시 보호 조치	4.4.1 파기규정 및 절차	O (다3.1.6)	X	보유기간 및 파기 관련 내부 규정 마련 휴면이용자의 경우, 개인정보 파기 예정고지와 파기조치 및 안내	O	O	O	O
	4.4.2 파기	O (다3.1.3 다3.1.5)	O (5.4.1 5.4.2)	수집 목적달성시, 안전한 방법으로 지체없이 파기, 파기에 관한 사항을 기록관리, 관련 법령 등에 의해 보유해야 한다면 〈정보주체〉에게 보유근거, 목적,기간 ,항목을 고지하고 최소한으로 보유	O	O	O	O
	[요구사항] · 개인정보에 보유기간을 설정하고 보유만료 전 개인정보만 검색가능해야함 · DB, 서버, PC, 모바일, USB내 개인정보를 복구재생이 불가한 방법으로 파기			[필요솔루션] 개인정보보유현황분석&파기 DB, 서버 내 개인정보 Server-i PC, 모바일 내 개인정보 Privacy-i				

5. 정보주체 권리보장 (3개 항목)

항목	기준	기존 인증기준 내 동일항목 존재여부		상세내용	적용대상			
		기존PIMS	PIPL		공공	대기업	중소기업	소상공인
5.1 정보 주체 권리 보장	5.1.1 열람/정정/ 삭제 요구	O (다2.2.2 다2.2.4)	O (6.1.1)	〈정보주체〉의 요구(열람/정정/삭제요구, 삭제방법 및 절차 정보제공요구) 시 지체없이 처리 및 기록, 법령에 따라 [개인정보 이용내역] 주기적통지	O	O	O	O
	5.1.2 처리정지 요구	O (다2.2.3)	O (6.1.2)	〈정보주체〉의 요구(처리정지 방법 / 절차 제공,처리정지 요구) 시 지체없이 처리, 기록	O	O	O	O
	5.1.3 권리행사 방법/ 절차	O (다2.2.1)	O (6.1.3)	〈정보주체〉가 열람 등 요구에 대한 거절 등 조치에 이의를 제기할 수 있도록 상담창구 등 필요한 절차 마련	O	O	O	O
	[요구사항] 정보주체를 식별할 수 있도록 〈Whose Privacy, 누구의 개인정보〉를 접근 , 이용하는지 기록			[필요솔루션] 개인정보처리시스템접근기록솔루션 DB DB-i WAS WAS-i				

〈통합 PIMS인증〉 중 기술적 보호조치 외 나머지 항목 7/9

6. 관리적보호조치 (12개 항목)

항목	기준	기존 인증기준 내 동일항목 존재여부		상세내용	적용대상			
		기존PIMS	PIPL		공공	대기업	중소기업	소상공인
6.1 교육/훈련	6.1.1 교육 / 훈련 시행·평가	O (나4.1.1 나4.1.2 나.4.2.1)	O (7.2.2)	〈연간 개인정보보호교육 계획〉 수립(시기, 기간, 대상, 내용, 방법 등 포함) → 임직원, 외부자 대상 연 1회 이상 교육 시행 → 시행기록 → 결과 평가 → 다음 교육에 반영	O	O	O	O
6.2 〈취급자〉 관리	6.2.1 취급자 감독	O (나5.1.1)	O (7.3.1)	〈취급자〉최소지정, 목록화 등 〈보호대책〉 수립	O	O	O	O
	6.2.2 보안서약서	O (나5.1.2)	O (7.3.2)	보안서약서 받음 (임시직원 or 제3자 등에게 접근권한부여시에도 받음)	O	O	O	O
	6.2.3 퇴직/직무 변경관리	O (나5.1.3)	O (8.1.2)	관련부서(인사부서, 개인정보보호/ 시스템운영부서 등) 의 〈이행절차〉 수립 (자산반납, 접근권한회수·조정, 결과 확인 등)	O	O	O	O
6.3 위탁 업무 관리	6.3.1 위탁계약	O (다2.3.3)	O (7.4.1)	외부위탁시 요구사항 / 관리감독사항을 계약서 등에 문서화, 수탁자의 법규정위반에 대한 〈처리절차〉 수립	O	O	O	O
	6.3.2 〈정보주체〉 고지	O (다2.3.1 다2.3.2)	O (7.4.2)	수탁자, 수탁목적 등 관련사항을 정보주체에게 고지, 필요시 동의획득	O	O	O	O
	6.3.3 위탁자 관리·감독	O (다 2.3.4)	O (7.4.3)	위탁업체가 계약서 / 서비스 수준 협약, 법 · 규정을 이행하는지 주기적관리 · 감독	O	O	O	O
6.4 침해 사고 관리	6.4.1 대응절차 수립 / 훈련	O (나6.1.1 나6.2.1)	O (7.5.1)	긴급연락체계, 보고 / 대응, 사고대응조직구성 등을 포함한 〈침해사고 대응절차〉 수립,시나리오에 따른 모의훈련 실시	O	O	O	
	6.4.2 대응체계 구축	O (나6.2.1)	O (7.5.1)	신속한 침해사고 대응을 위해 중앙 집중적 대응체계구축 외부기관 / 전문가와의 협조체계 수립	O	O	O	O
	6.4.3 보고 /처리·복구	O (나6.2.2. 나6.2.3)	O (7.5.2)	침해사고 징후 or 사고발생 인지시 〈유형별 보고절차〉에 따라 신속히 보고, 법적통지 / 신고의무 준수, 〈대응절차〉에 따라 신속히 처리, 복구	O	O	O	O
	[요구사항] · 외부에서 접근가능한 웹서버가 DB와 연계연동하여 누구의 개인정보에 접근하는지 기록한다 · 네트워크, 출력물, USB를 통하여 어떤 정보가 외부로 나가는지 기록하고 정책 이상 정보유출시 경보한다			[필요솔루션] Endpoint DLP Privacy-i Network DLP Mail-i				
	6.4.4 분석/정보 공유	O (나6.3.1)	X	개인정보침해사고 처리→ 종결 → 분석 → 결과보고 →정보와 취약점들을 관련 조직 / 임직원들과 공유	O	O		
	6.4.5 재발방지	O (나6.3.2)	X	유사 침해사고가 반복되지 않도록 〈재발방지 대책〉 수립, 필요시 정책, 절차, 조직 등의 대응체계 변경	O	O		

〈통합 PIMS인증〉 중 기술적 보호조치 외 나머지 항목 8/9

8. 물리적 보호조치(9개 항목)

항목	기준	기존 인증기준 내 동일항목 존재여부		상세내용	적용대상			
		기존PIMS	PIPL		공공	대기업	중소기업	소상공인
8.1 영상정보처리기기 관리	8.1.1 설치·운영 제한	O (나8.3.1)	O (9.1.1)	설치 목적에 따라 법적 요구사항(안내판 설치 등)을 준수, 적절한 보호조치 마련	O	O	O	O
	8.1.2 설치·운영 사무 위탁 관리	X	O (9.1.2)	적절한 위탁절차 마련	O	O	O	
8.2 물리적 보안 관리	8.2.1 보호구역의 지정, 관리	O (나8.1.1 나8.1.2)	X	· 비인가자의 물리적접근, 환경재난으로부터 보호하기 위하여 보호구역 (통제구역, 제한구역, 접견구역 등) 지정, 〈보호대책〉 수립·이행 · 온습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 설비를 갖추고 〈운영절차〉수립,운영, · 주요 〈개인정보처리시스템〉을 외부 집적정보통신시설에 위탁운영 시 관련 요구사항을 계약서에 반영, 주기적 검토	O	O	O	O
	8.2.2 출입통제 / 사무실 보안	O (나8.1.4 나8.2.2)	O (9.2.1)	보호구역에 인가자만 접근할 수 있도록 출입 통제, 출입 / 접근이력 주기적으로 검토, 공용사무처리기기, 문서고, PC, 파일서버 등에 보호대책 마련	O	O	O	O
	8.2.3 개인 업무 환경 보안	O (나8.2.1)	O (9.2.1)	자리비울 경우 책상 위에 중요문서나 저장매체 남겨놓지 않고, 화면보호기 설정, 패스워드 노출 금지 등 보호대책 수립	O	O	O	O
	8.2.4 이동컴퓨팅 보안관리	O (나8.1.5)	O (9.2.2)	(노트북 등) 미승인기기 반/출입을 통한 정보유출, 내부망 악성코드감염 예방을 위해 보호구역 내 임직원 / 외부자 대상 〈모바일 기기 반·출입 통제절차〉 수립, 기록·관리	O	O	O	

〈통합 PIMS인증〉 중 기술적 보호조치 외 나머지 항목 9/9

8. 물리적 보호조치(9개 항목)

항목	기준	기존 인증기준 내 동일항목 존재여부		상세내용	적용대상			
		기존PIMS	PIPL		공공	대기업	중소기업	소상공인
8.3 매체 / 출력물 관리	8.3.1 저장매체 관리	O (나7.4.1 나7.4.2)	O (9.2.3 9.2.4)	〈개인정보처리시스템〉,매체의 취급·보관, 폐기, 재사용 절차 수립, 폐기/ 재사용시 개인정보는 완전삭제, 매체(외장하드, USB, CD)는 악성코드감염방지대책 마련	O	O	O	
	[요구사항] · 개인정보처리시스템 및 매체에 어떤 개인정보가 있는지 식별한다 · 매체의 개인정보를 복구 재생이 불가한 방법으로 파기한다 · 허용되는 USB목록을 관리한다 허용되지 않은 USB가 PC에 연결되는 것을 차단한다			[필요솔루션] 개인정보보유현황분석&파기 DB, 서버 내 개인정보 Server-i PC, 모바일 내 개인정보 Privacy-i				
	8.3.2 저장매체 보관	X	O (9.2.5)	개인정보포함 저장매체를 안전한 장소에 보관	O	O	O	
	[요구사항] · 개인정보포함매체가 무엇인지 식별할 수있도록 관리한다 · 매체에 개인정보복제시마다 기록한다 · 정책이상의 개인정보가 매체로 복제되는것을 차단한다			[필요솔루션] 엔드포인트DLP Privacy-i				
	8.3.3 출력, 복사 통제	O (나7.7.1)	X	출력시 용도특정, 출력 항목 최소화 출력방법(테이프, 디스크, 인쇄, 휴대용 저장매체 등)에 따라 보호대책 수립- 출력 일시, 방법 등 기록·관리 등	O	O		
	[요구사항] · 개인정보 출력시 결재를 통해 용도를 확인한다 · 정책이상 대량출력시 차단한다 · 출력시 jpg와 text로 로그를 남겨서 원본을 확인하는 동시에 로그를 검색할 수 있도록 한다			[필요솔루션] 엔드포인트DLP Privacy-i				

04

전자금융거래법고시

전자금융감독규정

(적용대상 : 금융회사 · 전자금융업자)

발송일
2015. 06

2015년 4월 16일부터 시행중입니다

금융감독원
〈전자금융감독규정 시행세칙〉 일부개정안①

전자금융감독규정 시행세칙 개정안 원문보기

적용대상: 금융회사 및 전자금융업자(전자금융관련 자금이체, 직/선불지급수단 발행관리, 결제대행업)
시행일자: 2015.04.16

① 외주 보안관리 책임 확대 및 구체화

외주단계별로 〈보안관리방안〉 31개 항목 준수

일 1회 외주인력 대상으로 〈중요점검사항〉 12단계 점검

② 보안의 최종책임자는 CEO임을 명시

CEO는 CISO로부터
34개 보안점검결과를 매월 보고받아야 함

월 1회 〈정보보안 점검의 날〉 지정 ▶ 〈정보보안 점검항목〉 34개 항목 점검 ▶ CEO에게 〈점검결과/보완계획〉 보고

〈전자금융감독규정〉 개정, 외주관리 책임확대

〈전자금융감독규정〉 60조 (외부주문 등에 대한 기준)

① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문(=외주) 등의 경우에는 다음 각 호의 사항을 준수하여야 한다.

7. 외부주문등의 입찰 · 계약 · 수행 · 완료 등 각 단계별로 금융감독원장이 정하는 〈보안관리방안〉을 따를 것

14. 외부주문등은 자체 보안성검토 및〈정기 보안점검〉 실시 금감원장이 정하는 〈중요점검사항〉은 매일 보안점검 실시

〈전자금융감독규정 시행세칙〉개정, CEO보고항목인 〈34개 점검항목〉구체화

신설 〈전자금융감독규정 시행세칙〉 9조의2 (외부주문 등에 대한 기준)

① 규정 60조 ①항 7호에 따라 감독원장이 정하는 〈보안관리방안〉은 〈별표 5-2〉와 같다

② 규정 60조 ①항 14호에 따라 감독원장이 정하는 〈(일일)중요점검사항〉은 〈별표5-3〉과 같다

1페이지로 보는 외주단계별〈보안관리방안〉 31개 항목

전자금융 감독규정 시행세칙 〈별표 5-2〉

외주단계		금융회사의 보안관리방안	기술적 보호조치
입찰		1. (공고 이전) 내부관리기준/법규 검토 후, 투입예상 자료/장비에 대한 보안요구사항 마련	
		2. (공고시) 중요정보, 부정당업자 제재조치, 기밀유지의무, 위반시 불이익 등을 정확히 공지	
		3. (제안서평가요소) 자료/장비/네트워크보안대책/중요정보관리방안 등 〈보안관리계획〉 평가, 배점기준 마련	
		4. (사업자선정시) 제안서 상의 〈보안관리계획〉 타당성을 검토하여 사업자 선정	
계약		5. (계약서 작성 초기단계부터) 〈정보보안사항〉 포함여부 검토	
		6. 대외보안상 필요시 보안범위,책임을 명확히 하기 위해 사업수행계획서와 별도로 〈비밀유지계약서〉 작성	
		7. 〈비밀유지계약서〉 포함사항: 비밀정보범위, 보안준수사항, 손해배상, 지재권, 자료반환 등	
		8. 금융회사 사전동의없이 용역업체가 용역참가인원을 교체할 수 없음을 명시	
		9. 과업지시서/계약서에 1) 인원/장비/자료 보안조치사항 2) 정보유출 손해배상내용 기술	
		10. 용역업체의 하도급계약시 원래 사업계약수준의 비밀유지조항을 포함하도록 조치	
		11. 〈전자금융 감독규정〉 제7조 각호에 규정한 사항 포함 1) 인력,조직,예산 2) 건물,설비,전산실 등 시설 3) 단말기,전산자료,정보처리시스템 및 정보통신망 등 정보기술부문 4) 그 밖에 전자금융업무의 안전성 확보를 위하여 필요한 사항	
수행	인력	12. 정보유출방지조항 및 자필서명포함 보안서약서 징구	
		13. (사업 전) 법, 내규에 따른 보안교육 실시 * 유출금지정보, 유출시 제재조치 포함	
		14. (사업수행 중) 용역업체인력 보안점검, 정보유출여부 확인	[DLP] Mail-i, Privacy-i
	자료	15. 계약서 명시 중요정보를 용역업체에 제공시 1) 자료관리대장 작성 2) 인계/인수자 직접 서명 후 제공 3) 사업완료시 회수	
		16. 사업자료/산출물은 금융회사 파일서버 or 지정된 PC에 저장관리	[EndpointDLP] Privacy-i
		17. 자료공유사이트(P2P, 웹하드 등) 및 개인메일함에 자료저장 금지 금융회사-용역업체간 메일전송시 1) 자체전자우편 이용 2) 중요정보는 암호화전송	[DLP] Mail-i, Privacy-i
		18. 금융회사제공 사무실에서 사업수행시 유출금지정보는 매일 퇴근시 시건장치 설치된 보관함에 보관	
		19. 사업수행 산출물/기록은 비인가자에게 제공/대여/열람 금지	[DLP] Mail-i, Privacy-i [비업무사이트접속차단] WebKeeper
	사무실/장비	20. 사업수행장소는 전산실 등 중요시설과 분리, CCTV/시건장치 등 출입통제대책 마련	
		21. 용역업무 수행공간 대상 정기적 보안점검	
		22. 용역직원이 외부노트북으로 내부망접속시 악성코드감염확인, 반출시 자료무단반출 확인	[백신] [세이프브라우징] WebKeeper [EndpointDLP] Privacy-i
		23. 비인가 휴대저장매체(USB 등) 사용금지, 필요시 금융회사 승인	[EndpointDLP] Privacy-i
	내/외부망 접근시	24. 개발시스템-운영시스템 분리, 용역업체는 업무상 필요한 서버에만 제한적 접근	[개인정보처리시스템 접근통제] (DB) DB-i (WAS) WAS-i (SAP) App-i
		25. 용역업체 금융회사 전산망 접속 필요시 1) 사업참여인원 ID는 1개 그룹으로 등록 2) ID별 접근권한을 차등부여하여 내부문서 접근금지 3) 불필요시 즉시 해지 or 계정폐기 4) 내부서버/네트워크장비 접근기록 이상여부 정기점검 5) 참여인원계정은 별도 기록관리, 수시로 해당계정에 접속하여 저장자료/작업이력 확인	
		26. 용역업체 PC는 인터넷연결 금지, 필요시 금융회사 통제하에 제한적 허용	
		27. 용역업체 사용 전산망에는 자료공유사이트(P2P, 웹하드 등) 접속 원천차단	[비업무사이트접속차단] WebKeeper
완료		28. 최종 산출물 등 대외보안자료는 1) 대외비 이상으로 작성/관리 2) 불필요 자료 삭제/폐기	[개인정보검출삭제] Privacy-i
		29. 용역관련 제반자료(용역업체 제공자료,장비,산출물)는 1) 전량회수 2) 업체에 복사본 별도보관 금지	
		30. 용역업체소유 PC/서버의 전자기록 저장매체(하드디스크, USB 등)는 복원불가방법으로 완전삭제 후 반출	[디가우저] [문서파쇄기]
		31. 사업자료 회수/삭제 후 용역업체에게 '용역사업관련 자료 미보유' 확약서를 대표자 명의로 징구	

발송일
2015. 06

2015년 4월 16일부터 시행중입니다

금융감독원
〈전자금융감독규정 시행세칙〉 일부개정안②

전자금융감독규정 시행세칙 개정안 원문보기

적용대상: 금융회사 및 전자금융업자(전자금융관련 자금이체, 직/선불지급수단 발행관리, 결제대행업)
시행일자: 2015.04.16

① 외주 보안관리 책임 확대 및 구체화

외주단계별로 〈보안관리방안〉 31개 항목 준수

일 1회 외주인력 대상으로 〈중요점검사항〉 12단계 점검

② 보안의 최종책임자는 CEO임을 명시

CEO는 CISO로부터
34개 보안점검결과를 매월 보고받아야 함

월 1회 〈정보보안 점검의 날〉 지정 ▶ 〈정보보안 점검항목〉 34개 항목 점검 ▶ CEO에게 〈점검결과/보완계획〉 보고

〈전자금융감독규정〉개정, CEO는 매달 〈정보보안점검결과〉를 보고받아야 함

〈전자금융감독규정〉 37조의5 (정보보호최고책임자의 업무)

정보보호최고책임자(CISO)는 〈정보보안점검의 날〉을 지정하고,
임직원이 금융감독원장이 정하는 〈정보보안 점검항목〉을 준수했는지 여부를 매월 점검하고,
그 점검 결과 및 보완 계획을 최고경영자(CEO)에게 보고하여야 한다

〈전자금융감독규정 시행세칙〉개정, CEO보고항목인 〈34개 점검항목〉구체화

신설 〈전자금융감독규정 시행세칙〉 시행세칙 7조의3 (정보보호최고책임자의 업무)

규정 37조의5에 따라 감독원장이 정하는 〈정보보안 점검항목〉은 〈별표 3-2〉와 같다

CISO가 CEO에게 보고해야하는 34개 〈정보보안 점검항목〉

전자금융 감독규정 시행세칙 〈별표 3-2〉

구분	내용	기술적 보호조치
전산실	1. (상시출입자 외) 출입자에 대한 책임자승인 및 출입자관리기록부 기록보관	
	2. 무인감시카메라 or 출입자동기록시스템 정상작동	
단말기	3. (업무담당자 외) 단말기 무단조작 금지조치	
	4. 정보처리시스템 접속 단말기 사용자기록 유지	
	5. 중요 단말기 외부반출금지	
	6. 중요 단말기 인터넷 접속금지	망분리솔루션
	7. 중요 단말기 그룹웨어 접속금지	
	8. 보조기억매체/휴대용 전산장비 접근통제	[PC] Privacy-i [모바일] Smart-i
전산자료	9. 개인별 사용자계정, 비밀번호 부여	
	10. 사용자계정 및 비밀번호 등록/변경/폐기	
	11. 이용자정보 조회/출력통제	[개인정보 출력물 기록관리 및 통제] Privacy-i [개인정보처리시스템 접속기록관리/과다조회 통제] (DB)DB-i (WAS)WAS-i (SAP)App-i
	12. 테스트시 이용자정보 사용금지 및 불가피한 경우 1) 이용자정보 변환하여 사용 2) 테스트 종료 즉시 삭제	
	13. 단말기에 이용자정보 등 주요정보 보관금지 및 불가피한 경우 책임자 승인여부 확인	[Endpoint DLP] Privacy-i
	14. 단말기 공유금지	
	15. 전산자료 및 전산장비 반출/반입통제	[DLP] Mail-i, Privacy-i
	16. 사용자 인사조치시 지체없이 해당 사용자계정 사용중지, 삭제 공동사용계정변경 등 정보처리시스템 접근을 통제하고 있는지 확인	[DB접근통제솔루션] DB-i [서버접근통제솔루션]
정보처리시스템	17. 내부통신망의 비인가 전산장비/무선통신 접속통제	[NAC]
해킹 등 방지대책	18. 해킹방지 정보보호시스템 정상작동	[백신] [APT] [세이프브라우징] WebKeeper
	19. 정보보호시스템에 최소 서비스번호/기능 적용	
	20. 정보보호시스템에 업무목적이외 기능/프로그램 제거	
	21. 정보보호시스템 원격관리금지	[터미널서비스 접속차단] WebKeeper
	22. 긴급하고 중요한 보정사항에 대한 보정작업 즉시 실시 여부	
	23. 무선통신망 이용업무 승인/사전지정	
악성코드	24. 악성코드검색/치료 프로그램 최신상태 유지	[백신] [APT] [PMS] [세이프브라우징] WebKeeper
	25. 중요 단말기의 악성코드 감염여부 일 1회 점검	[백신]
공개용 웹서버	26. 사용자계정에 아이디/비밀번호 이외 추가인증수단 적용	
	27. DMZ구간 내 이용자정보 등 주요정보 저장/관리	[서버개인정보검출삭제] Server-i
내부사용자 비밀번호	28. 접근자 비밀번호 설정/운영	
	29. 비밀번호 보관시 암호화	
이용자 비밀번호 관리	30. 정보처리시스템/전산자료 내 이용자 비밀번호 암호화보관	
이용자 유의사항	31. 비밀번호 유출위험 및 관리사항 공지	
	32. 제공 중인 이용자보호제도 공지	
	33. 해킹/피싱 등 전자적 침해방지사항 공지	
전자금융사고 보고	34. 전자적 침해행위 보고/조치	

〈금융분야 개인정보유출 재발방지 종합대책〉에서 예고한

〈외주용역 일일체크리스트〉 외주업체 중요점검사항 12단계

전자금융 감독규정 시행세칙 〈별표 5-3〉

단계	점검항목	기술적 보호조치
1	이용자 정보 조회/출력 통제 및 이용자 정보 조회시 사용자, 사용일시, 변경조회내역, 접속방법 기록관리	[개인정보 출력물 기록관리 및 통제] Privacy-i [개인정보처리시스템 접속기록관리/과다조회 통제] (DB) DB-i (WAS) WAS-i (SAP) App-i
2	테스트시 이용자 정보 사용금지 부하 테스트 등 사용이 불가피한 경우 1) 이용자정보 변환사용 2) 테스트 종료 즉시 삭제	[개인정보검출삭제] Privacy-i [개인정보변환솔루션]
3	운영시스템 접속 및 사용통제	[DB접근통제솔루션] DB-i [서버접근통제솔루션]
4	내부통신망의 비인가 전산장비/무선통신 접속통제	
5	전산자료 및 전산장비 반출입통제	[DLP] Mail-i, Privacy-i
6	전산실 등 출입자 관리기록부 기록/보관	[물리적 출입통제]
7	인터넷(무선통신망 포함) 사용통제	[비업무사이트접속차단] WebKeeper
8	업무담당자 외 단말기 무단조작금지	[2채널 인증강화된 사용자인증]
9	운영체제 및 악성코드 치료프로그램 최신유지	[백신] [세이프브라우징] WebKeeper
10	USB 등 보조저장매체 사용통제	[Endpoint DLP] Privacy-i
11	단말기에 이용자 정보 등 중요정보 보관금지	[개인정보검출삭제] (PC) Privacy-i (서버) Server-i
12	정보처리시스템 개발업무에 사용되는 장소 및 전산설비를 내부용과 분리하여 설치운영, 비인가자 출입통제	

05

의료기관 · 약국의

개인정보보호 변화

(적용대상 : 의료기관 · 약국)

〈의료기관 · 약국〉 개인정보보호 어떤 변화가 진행중인가?

사고

① 2015년 1월 검찰적발
외주전산업체가 〈의료기관 · 약국〉의
4,400만명 개인정보 외부전송
건강보험청구 SW〈외주전산업체〉가
2011~14, 3년간
의료기관/약국18,300곳에서
개인정보 47억건을 외부전송,
비식별화하여 〈글로벌 통계회사〉에 판매

대책

② 2015년 7월 보건복지부, 재발대책 발표
2015년 7월 23일
〈의료기관 · 약국의 환자 개인정보 보호대책〉 발표

점검

〈의료기관 · 약국〉 개인정보자율점검
2015년 10월말까지 신청완료
2016년 4월 30일까지 보완완료

③ 의료기관 64개 체크리스트
〈대한병원협회〉 주관으로
회원의료기관 2,849곳 자율점검

④ 약국 40개 체크리스트
〈대한약사회〉주관으로 회원약국 자율점검

⑤ 약국 40개 체크리스트에서 뽑은
개인정보보호 Q&A

법개정

민감정보에 개인정보보호법고시 〈개인정보의 안전성 확보조치 기준〉 적용 강화 13p

미조치로 민감정보 유출시
형사처벌
몰수추징
손해배상

〈의료기관 · 약국〉의 개인정보보호 특별법인
〈건강정보보호법〉 탄생 예고

개정 예정 규정:
〈국민건강보험법〉
〈의료기관 개인정보보호 가이드라인〉
〈약국 개인정보보호 가이드라인〉

쟁점

산업발전을 위한 빅데이터 활용인가? VS 영리목적의 개인정보유출사고인가?

대형소송 진행중

외주전산업체와
글로벌통계회사 4개사와
CEO 포함 24명 검찰기소
현재 김앤장, 태평양, 화우
변호로 재판중

비식별화했으므로 개인정보가 아닌가? VS 다른정보와 결합,식별가능하므로 개인정보인가?

산업발전을 위한 글로벌 정보공유인가? VS 영리목적의 해외유출인가?

(클라우드에 의료빅데이터를 저장, 활용해야 하는)
원격의료사업에 어떤 영향을 미칠 것인가?

발송일
2015. 11

외주전산업체가 〈의료기관 · 약국〉 18,300곳에서 4,400만명 개인정보 47억건 외부전송!

2015 〈의료기관 · 약국〉 개인정보보호 어떤 변화가 진행중인가?

사고

2015년 1월 검찰
외주전산업체의 의료기관 · 약국
환자 개인정보 불법처리사건 적발

2008.3~2014.12
병원 7,500곳에서

2011.1~2014.11
전체 약국의 절반인
약국 10,800곳에서

외주전산업체
(전자차트, 건강보험청구SW, 약국경영관리SW)
개인정보 불법수집 후 판매

환자이름, 생년월일,
병명, 약물명, 복용량 등

진료정보 4억3,019만건을
3억3천만원에 판매

환자이름, 주민번호,
병명, 조제/투약내용 등

처방정보 43억3,593만건을
16억원에 판매

〈다국적 의료통계 회사〉
개인정보 구입 후
약 4,400만명의 개인정보를
통계화하여 제약회사에 70억원에 판매

쟁점

의료법, 개인정보보호법,
정보통신망법 위반
의료빅데이터 활용 및
국외유출이라는 쟁점 발생

대책

2015년 7월 보건복지부 재발대책
〈의료기관 · 약국의 환자 개인정보 보호대책〉 중
긴급대책에 해당하는 부분

해당 건강보험
청구SW 사용금지
(의료기관A사 , 약국 D재단)

행자부, KISA, 심평원 합동
유출관련 외주4개사 긴급점검

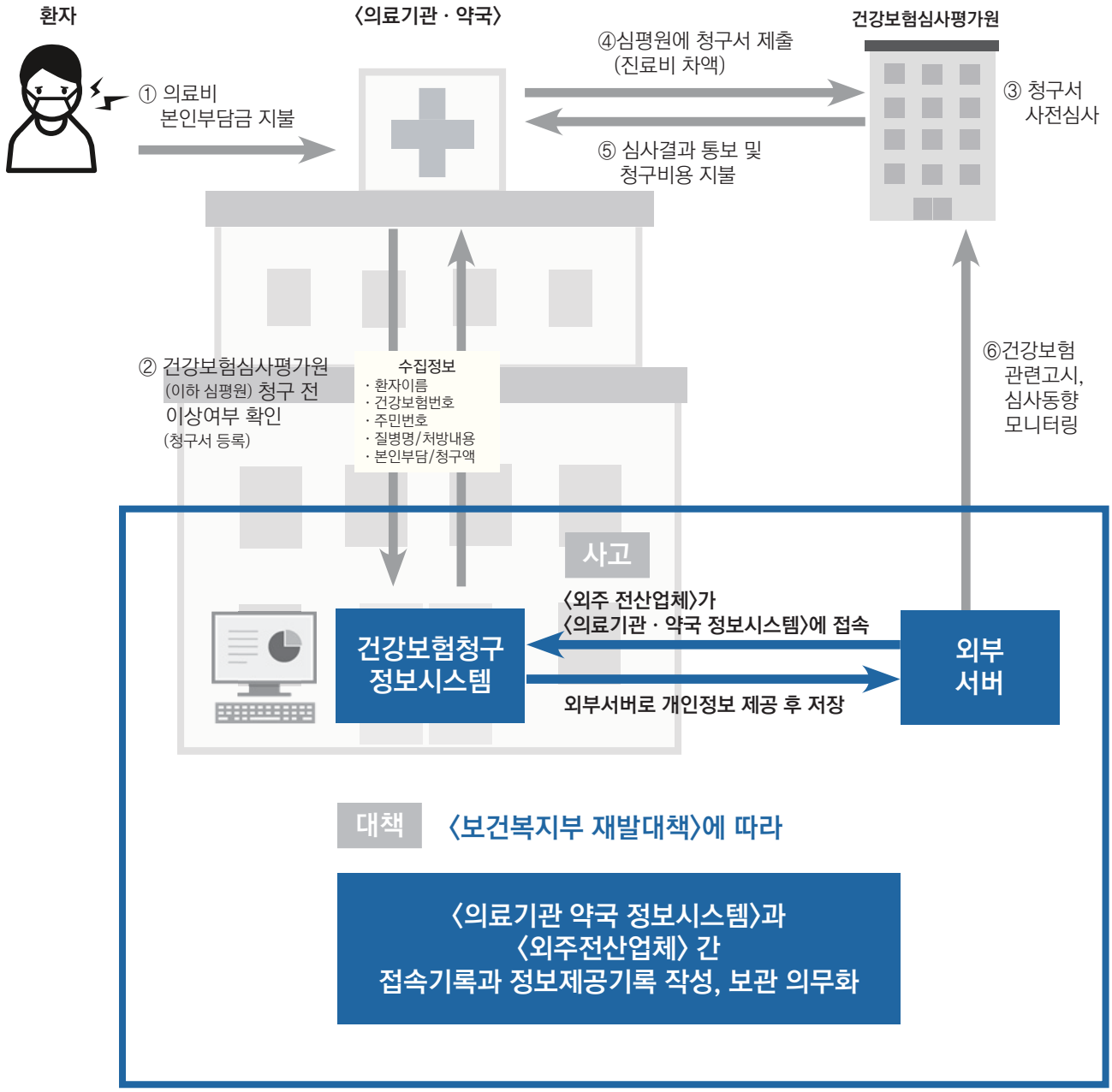
**불법취득한 환자 개인정보를
파기했는지 집중점검**

의료기관 약국 7만곳의
개인정보를 처리하는
외주 전산업체 27개사 점검

행정자치부, 보건복지부에서
2014년 3개사,
2015.2월 9개사, 5월 15개사 점검

사고

외주전산업체가 〈의료기관 · 약국〉 정보시스템에 접속, 외부서버로 정보전송



대책

2015년 7월 보건복지부 재발대책
〈의료기관 · 약국의 환자 개인정보 보호대책〉 발표

의료기관 · 약국 관리감독 강화

점검

① 500여개 병원급 의료기관, **행정자치부 주관 합동점검** 실시

② 나머지 의료기관 · 약국 **〈의료인단체〉 중심으로 자율점검** 실시

심평원 요양기관대상 자율점검
대한병원협회 회원병원대상 자율점검
대한약사회 회원약국대상 자율점검

③ 점검결과를 분석하여 개선방안 마련

교육

의료인 · 약사 **보수교육과정에 정보보호교육** 강화

규정 개정예정
〈의료기관 개인정보보호 가이드라인〉
〈약국 개인정보보호 가이드라인〉

건강보험 청구SW 관리감독 강화

점검

사전인증및 사후검사항목에 **개인정보보안항목** 추가 (암호화, 불법처리방지등)

개인정보 **불법처리시 인증취소 및 (일정기간) 재인증 금지**

교육

〈건강보험 청구 S/W〉의 기능, **운영방식의 범위와 한계를 명확하게 설정**

건강보험 급여비용 청구자료 사전점검 및 **심평원의 청구심사결과를 사후 분석**하는 컨설팅 제공

규정 개정예정 〈국민건강보험법〉

외주전산업체 관리감독 강화

〈외주 전산업체 등록제〉 도입

〈외주 전산업체〉가 〈의료기관 · 약국 정보시스템〉에 접속한 기록과 〈의료기관 · 약국〉에서 **외부로 정보를 제공한 기록**을 **작성 · 보관토록 의무화**하여 불법정보유출 · 제공을 쉽게 확인

〈의료기관 · 약국용 정보시스템〉 대상으로 적격성 기준심사 후 **인증부여 및 인증받은 제품만 사용가능**
〈적격성 기준〉 기능성, 상호운영성, 보안성(기술적 관리적 보안성)

등록업체와 인증제품에 대한 **무작위 수시 점검체계 (Spot Check) 도입**

규정 개정예정 환자개인정보를 불법수집한 외주 전산업체 등에 대해서는 징벌적 과징금 등 엄격한 제재방안 마련

발송일
2015. 11

2015년 10월 말까지 신청완료, 2016년 4월 30일까지 보완완료

〈대한병원협회〉 주관
〈의료기관 자율점검 64개 체크리스트〉

의의

의료기관 개인정보보호에 있어 **가장 구체적인 2대 문서** 중 하나
다른 하나는 〈의료기관 개인정보보호 가이드라인〉(2015.2.3 개정)

자율점검 일정

강제성은 없으나 〈자율점검〉 미참여시 행정자치부 〈현장점검 리스트〉에 올라가게 됨

심평원 〈자율점검지원 시스템〉 접속

2015년 10월 31일까지
의료기관
〈자율점검 신청서〉 작성

→ 심평원 승인

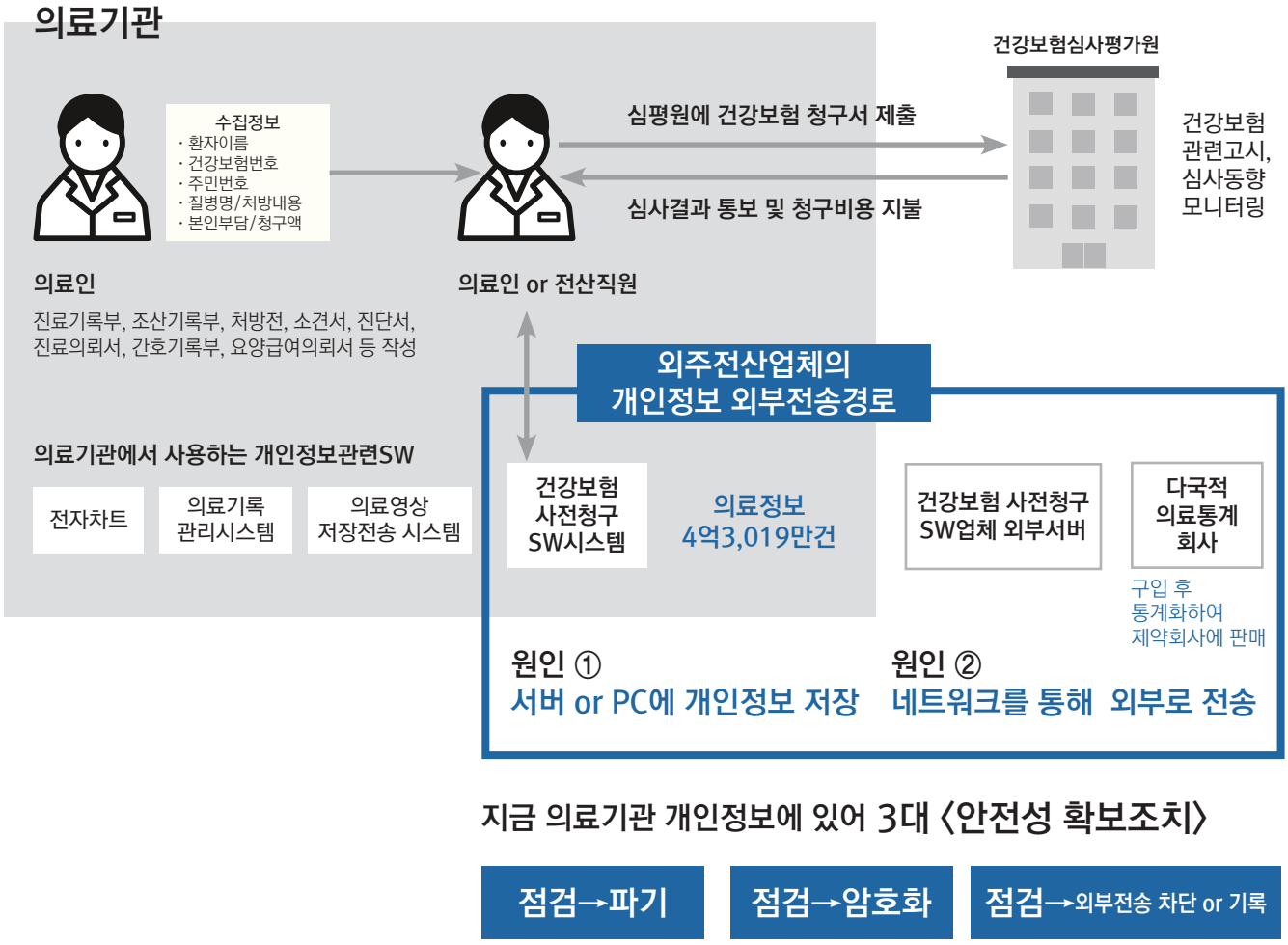
→ 의료기관
〈자율점검 64개 체크리스트〉의 각 항목별로 〈양호〉〈개선필요〉〈취약사항〉으로 체크하여 자료제출

→ 심평원 검토

→ 2016년 4월 30일까지
의료기관
〈자율점검 64개 체크리스트〉 상의 〈개선필요〉〈취약사항〉 보완 완료

2008.3~2014.12 **외주전산업체**가
병원 7,500곳에서
환자이름, 생년월일, 병명, 약물명, 복용량 등
진료정보 4억3019만건 외부전송, 3억3천만원에 판매

외주전산업체의 병원 내 개인정보 외부전송 경로는?



지금 의료기관 개인정보에 있어 3대 〈안전성 확보조치〉

점검→파기 | **점검→암호화** | **점검→외부전송 차단 or 기록**

〈의료기관 자율점검 64개 체크리스트〉 1/2

1. 개인정보보호법고시 〈개인정보의 안전성 확보조치〉에 따른 30개 항목

분야		체크리스트 포함 내용	기술적 보호조치
21조 파기		1. 보유기간 경과, 치리 목적(제공받은 경우 제공받은 목적) 달성 후 지체 없이 개인정보 파기 여부	[PC내 개인정보파일 검출,삭제,암호화] Privacy-i [서버내 개인정보파일 검출,삭제,암호화] Server-i
		2. 개인정보 파기 시 복구 또는 재생되지 않도록 조치 여부	
		3. 임시파일 및 출력자료 등에 대한 즉시 파기 여부	
		4. 법령에 따라 보존할 경우 별도 분리 보관 여부	
29조	내부 관리계획 수립시행	5. 내부관리계획 수립/시행 여부	
		6. 내부관리계획의 필수 반영사항(4개*) 포함 여부 * 4개 : 보호책임자지정, 보호책임자/취급자 역할/책임, 안전성확보조치, 취급자 교육	
	접근권한 관리 및 접근통제	7. 시스템 접근권한을 필요 최소한의 범위로 업무담당자에 따라 차등 부여 여부	[DB] DB-i [WAS] WAS-i [SAP] App-i
		8. 전보/퇴직 등 인사이동으로 취급자 변경시 접근권한 변경 또는 말소 여부	
		9. 접근권한의 부여/변경/말소 내역의 기록관리 및 최소 3년간 보관 여부	
		10. 취급자별로 개별 계정 발급 여부	
		11. 안전한 비밀번호 작성규칙의 수립/적용 여부	
		12. 불법접근, 침해사고방지를 위한 시스템 설치/운영 여부	
		13. 외부에서 정보통신망을 통한 접속시 가상사설망, 전용선 등 안전 접속수단 제공여부	
		14. P2P, 웹하드 등 비인가 프로그램, 공유 설정 등에 대한 접속 차단 실시 여부	[Endpoint DLP] Privacy-i [Network DLP] Mail-i
		15. 인터넷 홈페이지의 개인정보 노출 방지를 위한 보안조치 실시 여부	[웹서버내 개인정보 보유현황파악] Server-i
	암호화	16. 개인정보 암호화계획 수립/시행 여부	
		17. 비밀번호의 외부 송/수신 시 암호화 조치 여부	[PC내 개인정보파일 검출,삭제,암호화] Privacy-i [서버내 개인정보파일 검출,삭제,암호화] Server-i [DB암호화 솔루션] [전송구간 암호화 솔루션]
		18. 비밀번호의 내부 저장 시 일방향 암호화 조치 여부	
		19. 바이오정보의 외부 송/수신 시 암호화 조치 여부	
		20. 바이오정보의 내부 저장 시 암호화 조치 여부	
		21. 고유식별정보의 외부 송/수신 시 암호화 조치 여부	
		22. 고유식별정보의 인터넷과 내부망의 중간지점(DMZ) 저장시 암호화 조치 여부	
		23. 고유식별정보의 내부 저장시 암호화 조치 또는 그에 상응하는 조치 적용 여부	
	접속기록 보관	24 취급자의 접속기록을 최소 6개월 이상 보관/관리 여부	[DB] DB-i [WAS] WAS-i [SAP] App-i
		25. 접속기록의 항목(4개*)이 적정한지 여부 * 4개 : ID, 날짜 및 시간, 접속자 IP 주소, 수행 업무	
		26. 접속기록이 위/변조 및 도난, 분실되지 않도록 접속기록의 안전 보관 여부	
	보안 프로그램 설치운영	27. 보안 프로그램의 설치/운영 여부	[치료] 백신 [세이프브라우징] Webkeeper
		28. 보안 프로그램 자동 업데이트 또는 일 1회 이상 업데이트 실시 여부	
	물리적 접근방지	29. 전산실,자료보관실 등 물리적 보관 장소에 대한 출입통제절차 수립/운영 여부	Privacy-i 개인정보가 보조저장매체, 서류로 복제되는 것을 최소화함으로써 물리접근방지대상 최소화
		30. 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소 보관 여부	

〈의료기관 자율점검 64개 체크리스트〉 2/2

2. 그 외 34개 항목

분야	체크리스트 포함 내용
15조 수집이용시 동의	1. 온/오프라인 회원가입 시 동의 여부
	2. 각종 게시판, 기타 개인정보 수집 시 동의 여부
	3. 정보주체 동의 시 필수 고지항목(4개*) 고지 여부
	4. 필수 고지항목(4개*) 내용의 적정 여부 * 4개 : 목적, 항목, 보유 및 이용기간, 거부권 및 불이익
16조 최소수집	5. 목적에 필요한 최소한의 개인정보 수집 여부
	6. 최소한 정보 외의 개인정보 수집에 대한 미동의를 이유로 재화 또는 서비스 제공 거부 여부
17조 제공	7. 제3자에게 개인정보 제공 시 정보주체 동의 여부
	8. 정보주체 동의 시 필수 고지항목(5개*) 고지 여부
	9. 필수 고지항목(5개*) 내용의 적정 여부 * 5개 : 제공받는 자, 목적, 항목, 보유 및 이용기간, 거부권 및 불이익
18조 이용제공 제한	10. 개인정보 수집 당시 정보주체의 이용/제공 동의 범위를 초과하여 이용/제공 여부
	11. 개인정보 제공 시 제공 목적범위 내 이용, 안전 조치 실시, 목적 달성 후 파기 등 요청 여부
	12. 동의에 의한 목적 외 이용, 목적 외 제3자 제공 시 필수 고지항목(5개*) 고지 여부
	13. 필수 고지항목(5개*) 내용의 적정 여부 * 5개 : 제공받는 자, 목적, 항목, 보유 및 이용기간, 거부권 및 불이익
22조 동의받는 방법	14. 동의 사항의 구분 동의 여부
	15. 동의가 필요한 정보(필수정보)와 동의 없이 처리할 수 있는 정보(선택정보)의 구분 동의 여부
	16. 홍보 권유에 활용하기 위한 정보와 그렇지 않은 정보의 구분 동의 여부
	17. 선택항목 및 홍보 권유 정보의 미동의를 이유로 재화 또는 서비스 제공 거부 여부
23조 민감정보의 처리제한	18. 사상, 정치, 건강 등 민감정보의 동의에 의한 수집 및 제공시 구분 동의 여부
	19. 정보주체 동의시 필수고지항목(수집 4개, 제공 5개) 고지 여부
	20. 필수 고지항목(4개 또는 5개) 내용의 적정 여부
24조 고유식별정보 처리제한	21. 고유식별정보* 동의에 의한 수집제공 시 구분동의 여부 * 고유식별정보 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호
	22. 주민등록번호 외 회원가입 방법 제공 여부
26조 업무위탁에 따른 처리제한	23. 문서(계약서)에 필수 반영사항(6개*) 포함 여부 * 6개 : 목적외 처리금지, 기술/관리적 보호조치, 목적/범위, 재위탁 제한, 접근제한 등 안전조치, 관리/감독사항
	24. 수탁자 공개 여부
	25. 수탁자에 대한 교육 실시 여부
	26. 처리현황 점검 등 수탁자 관리/감독 여부
28조 개인정보 취급자 감독	27. 개인정보취급자에 대한 관리/감독(접근권한 관리, 통제 등 포함) 여부
	28. 개인정보취급자에 대한 보안서약서 징구 여부
	29. 개인정보취급자에 대한 정기적인 교육 실시 여부
30조 개인정보 처리방침의 수립/공개	30. 개인정보 처리방침의 수립 여부
	31. 개인정보 처리방침에 필수 항목(8개*) 포함 여부 * 8개 : 처리 목적, 처리 및 보유기간, 제3자 제공 사항(해당 시), 위탁사항(해당 시), 정보주체 권리/의무 및 행사 방법, 처리항목, 파기 사항, 안전성 확보 조치 사항
	32. 개인정보 처리방침의 홈페이지 등 공개 여부
31조 개인정보보호 책임자의 지정	33. 개인정보 보호책임자 지정 여부
	34. 개인정보보호책임자 업무범위, 자격요건 등 적정여부

64개 항목에는 없지만 의료기관이 준수해야하는 규정 1
개인정보보호법고시 〈개인정보의 안전성 확보조치 기준〉

분야	체크리스트 포함 내용	기술적 보호조치
3조 내부관리 계획의 수립시행	① 개인정보처리업무 위탁시 수탁자 관리감독	
5조 접근통제	③ 홈페이지에서 주민번호를 통한 본인확인시 추가인증수단 요구여부	
	⑤ 인터넷 홈페이지 취약점 연1회이상 점검	웹서버 내 개인정보 보유현황 파악 Server-i
7조 접속기록의 보관 및 점검	② 개인정보처리시스템 접속기록 반기별 1회 이상 점검	[DB] DB-i [WAS] WAS-i [SAP] App-I
9조 물리적 접근방지	③ 개인정보포함 보조저장매체 반출입통제 대책	Privacy-i 개인정보가 보조저장매체, 서류로 복제되는 것을 최소화함으로써 물리접근방지대상 최소화

64개 항목에는 없지만 의료기관이 준수해야하는 규정 2 〈의료기관 개인정보보호 가이드라인〉

<table>
<tr><th colspan="3">가이드라인 내 정보보호 규정</th><th>기술적 보호조치</th></tr>
<tr><td colspan="2">의료기관은
민감정보(환자건강상태, 신체특징, 병력),
주민번호, 고유식별정보,그 밖에
신용카드번호, 통장계좌번호, 근로정보,
개인영상정보 등
다양한 개인정보를 처리하고 있음

- 가이드라인 3p</td><td>개인정보취급자 범위는 정보주체의 개인정보
처리업무 수행자를 말하며 정규직 이외에
임시직, 파견근로자, 시간제근로자 등 포함(...중략)
개인정보취급자의 의무와 책임은 (...중략)
2. 개인정보의
기술적, 관리적 보호조치 기준 이행

- 가이드라인 129p</td><td rowspan="2">PC, 서버, DB까지
전사적
개인정보현황분석

[PC] Privacy-i
[서버] Server-i</td></tr>
<tr><td colspan="2">병원정보시스템, OCS, EMR, PACS, LIS,
건강검진시스템, 병원홈페이지 등
〈개인정보처리시스템〉에 사용자,직무,
그룹,역할별로 화면,메뉴,버튼
(읽기, 쓰기, 출력, 다운로드 등)단위의
상세접근권한을 설계하고 적용해야 함

- 가이드라인 77p</td><td>〈개인정보처리시스템〉 접속방법은 의사,
간호사 등이 병원정보시스템 등 응용시스템을
통해 접속하는 방법, DB관리자 등이 DB접속
툴을 이용하여 〈개인정보처리시스템〉에
접속하는 방법 등 다양한 방법이 존재하므로,
각 환경에 맞도록 접속기록을 남겨야 함

- 가이드라인 92p</td></tr>
<tr><td>개인정보다운로드
권한의 경우,
다운로드받은
파일에 의한
대량 개인정보유출이
가능하므로
권한 최소화

- 가이드라인 78p</td><td>업무용컴퓨터에 고유식별정보 등
개인정보저장시 분실, 고의, 실수,
악성코드 감염 등 다양한
위협요인에 따른 개인정보
유출위험이 매우 높으므로
업무용 컴퓨터내 개인정보 최소화

- 가이드라인 89p</td><td>의료기관은 보유기간 경과,
개인정보 처리목적달성 등
개인정보가 불필요할 때
지체없이 개인정보를 파기하고,
복구or재생되지 않도록
조치해야 함

- 가이드라인 96p</td><td>전사적
개인정보검출 및
복구or 재생되지
않도록
파기

[PC] Privacy-i</td></tr>
</table>

발송일
2015. 11

2015년 10월 말까지 신청완료, 2016년 4월 30일까지 보완완료

〈대한약사회〉 주관
〈약국 자율점검 40개 체크리스트〉

의의

약국 대상 최초의
개인정보
〈자율점검 체크리스트〉

약국현실을 반성한 구체성에 있어서
약국 개인정보 2대 문서 중 하나
다른 하나는 〈약국 개인정보보호 가이드라인〉 (2013.12.19 발간)

자율점검 일정

강제성은 없으나 〈자율점검〉 미참여시 행정자치부 〈현장점검 리스트〉에 올라가게 됨

심평원
〈자율점검지원 시스템〉 접속

2015년 10월 31일까지
약국
〈자율점검 신청서〉
작성

→ 심평원
승인

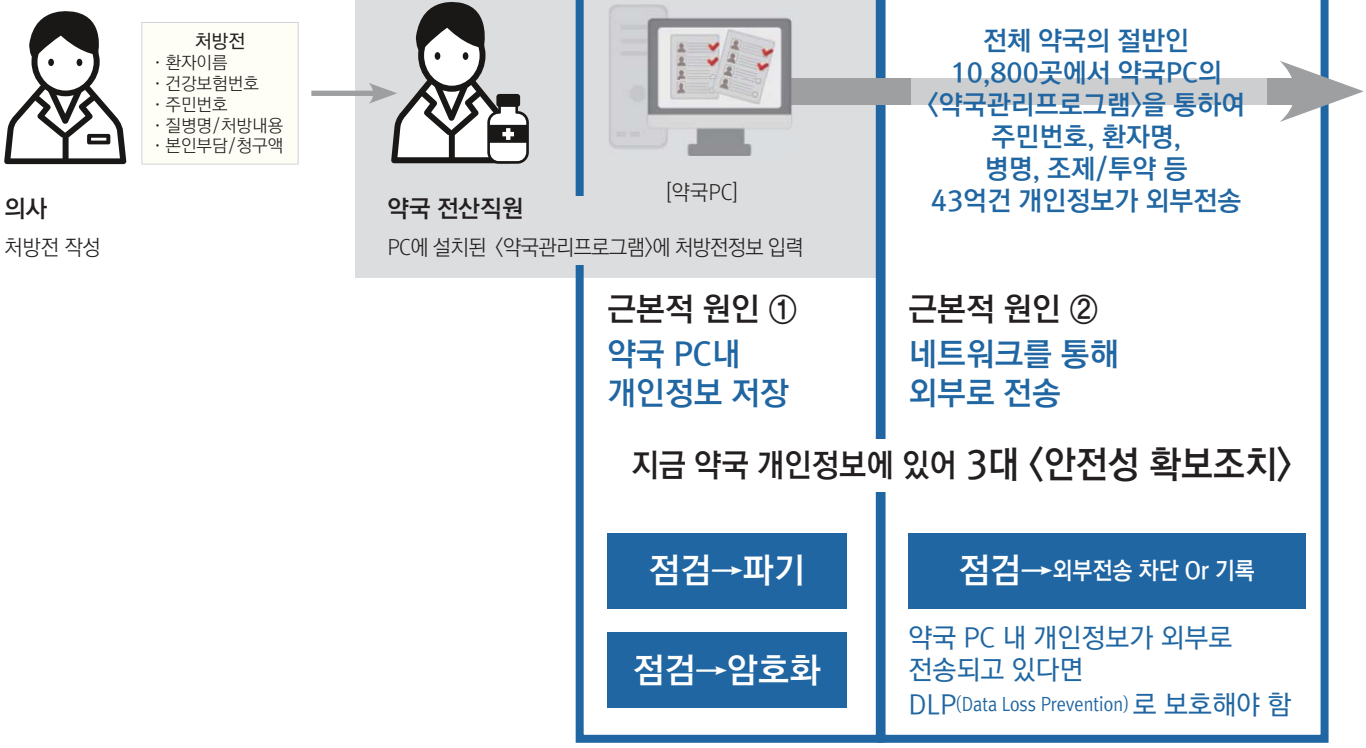
→ 약국
〈자율점검 체크리스트〉
40개 항목으로 실시

→ 심평원
검토

→ 2016년 4월 30일까지
약국
〈자율점검 체크리스트〉 상의
〈개선필요〉〈취약사항〉 보완 완료

약국 개인정보 유출사고 〈근본적 원인〉과 〈안전성 확보조치〉는 무엇인가?

〈병원〉



약국 개인정보보호 2대 문서에서 공통적으로 지적한 3대 〈안전성 확보조치〉

〈약국 자율점검 40개 체크리스트〉 대한약사회 2015년 10월 배포

점검→파기

체크리스트 7

보유기간경과, 목적달성 후 지체없이 개인정보를 파기하고 관리대장을 작성/관리하고 있는가?

〈양호〉등급을 받기 위한 제출문서
파기사실확인서, 사진 등 증빙자료 or 개인정보파기관리대장

체크리스트 8

개인정보 파기시 복구or재생되지 않도록 조치하고 있는가?

체크리스트 9

임시파일, 출력자료는 목적달성 후 즉시 파기하고 있는가?

〈양호〉등급을 받기 위한 제출문서
개인정보처리방침
or 내부관리계획

파기방법

개인정보가 약국청구프로그램 DB에 있을 경우 해당프로그램 기능으로 파기

이외 PC, 모바일, USB에 있을때는 파기솔루션 사용

점검→암호화

체크리스트 29

컴퓨터(PC)에 저장된 개인정보는
별도로 암호화 하고 있는가?

암호화대상

업무용 PC or
모바일기기에
저장된 주민번호포함
문서파일(hwp, xls, txt)

문서파일 암호화 방법

문서편집기에서 제공하는
암호설정기능 or 보안
프로그램 등에서 제공하는
파일 보안기능 활용

체크리스트 30

약국청구프로그램이 설치된 PC(=개인정보처리시스템)에
최신의 보안프로그램을 설치하여 관리하는가?

1. ID 공유금지 및 직원업무에 따라 접속권한부여
2. 약국관리프로그램에 로그인 비밀번호 설정
3. PC에 바이러스백신 설치 및 관리
4. PC에 방화벽 설정 및 관리
5. 비밀번호, 주민등록번호의 암호화 확인

보안강화를 위해 별도의
〈유료보안프로그램〉을
도입할 수 있음

〈양호〉등급을
받기 위한 제출문서
보안프로그램 계약서

점검→외부전송 차단 or 기록

체크리스트 40

(PC내) 개인정보 노출방지를 위해
점검프로그램 or 보안프로그램을 이용하여
(PC에서 외부로 개인정보가 노출된 내역을) 검사 등
모니터링 및 정기점검을 실시하고 있는가?

〈양호〉등급을 받기 위한 제출문서
개인정보 노출점검 리포트

〈약국 개인정보보호 가이드라인〉 보건복지부/행정자치부 2013년 12월 발간

점검→암호화

가이드라인 44p

약국PC에서 엑셀(xls), PDF 등 전자문서파일형태로
주민번호를 저장할 경우에는 상용암호화 SW로 암호화

외부전송 차단 or 기록

가이드라인 45p

유해사이트 차단프로그램 등을
사용하여 통제할 수 있음

〈약국 자율점검 40개 체크리스트〉

약국 유형 분류기준

구분	약국①	약국②	약국③	약국④
직원수	1~4인		5인 이상	
홈페이지or 서면을 통한 회원가입여부	X	O	X	O

체크리스트 포함 내용	약국유형별 적용여부			
	약국 ①	약국 ②	약국 ③	약국 ④
1. 온/오프라인 회원가입 시 동의 여부	X	O	X	O
2. 각종 게시판, 기타 개인정보 수집 시 동의 여부	X	O	X	O
3. 목적에 필요한 최소한의 개인정보 수집 여부	X	O	X	O
4. 최소한의 정보 외 개인정보 수집 미동의를 이유로 재화or서비스제공을 거부하는지 여부	X	O	X	O
5. 제3자에게 개인정보 제공 및 목적외 이용시 정보주체의 별도 동의 여부	O	O	O	O
6. 개인정보 제공 시 제공 목적범위 내 이용, 안전 조치 실시, 목적 달성 후 파기 등 요청 여부	O	O	O	O
7. 보유기간경과, 처리목적(제공받은 경우 제공받은 목적) 달성 후 지체없이 개인정보 파기여부	O	O	O	O
8. 개인정보 파기 시 복구 또는 재생되지 않도록 조치 여부	O	O	O	O
9. 임시파일 및 출력자료 등에 대한 즉시 파기 여부	O	O	O	O
10. 법령에 따라 보존할 경우 별도 분리보관 여부	O	O	O	O
11. 동의가 필요한 정보(필수정보)와 불필요한 정보(선택정보)의 구분 동의 여부	X	O	X	O
12. 만 14세 미만 아동의 개인정보 수집시 법정대리인 동의를 받고 있는지 여부	X	O	X	O
13. 홍보권유에 활용하기 위한 정보와 그렇지 않은 정보의 구분 동의 여부	X	O	X	O
14. 사상,정치,건강 등 민감정보의 동의에 의한 수집 및 제공시 구분 동의 여부	X	O	X	O
15. 고유식별정보의 동의에 의한 수집 및 제공 시 구분 동의 여부	X	O	X	O
16. 주민등록번호 외 회원가입 방법 제공 여부	X	O	X	O
17. 영상정보처리기기 운영 · 관리방침 수립 여부	O	O	O	O
18. 영상정보처리기기 설치장소에 필수기재사항을 포함한 안내판 설치 여부	O	O	O	O
19. 개인영상정보에 대한 이용 · 제공 · 열람 · 파기 내용 기록관리 여부	O	O	O	O
20. 개인영상정보가 분실 · 도난 · 유출 · 변조 · 훼손되지 않도록 안전성 확보조치 수립 여부	O	O	O	O
21. 위탁계약 시 문서(계약서)에 의한 계약 여부	O	O	O	O
22. 수탁업체에 대한 교육 및 처리현황 점검 등 관리 감독 실시 여부	O	O	O	O
23. 위탁에 관한 사실을 인터넷 홈페이지, 사보 등에 공개 여부	O	O	O	O
24. 개인정보취급자에 대한 보안서약서 징구 여부	O	O	O	O
25. 개인정보취급자 및 일반직원에 대한 정기적인 교육 실시 여부	O	O	O	O
26. 내부관리계획 수립/시행 여부	X	X	O	O
27. 연간 개인정보보호 교육계획 수립 여부	X	X	O	O
28. 안전한 비밀번호 작성규칙 적용 여부	O	O	O	O
29. 컴퓨터(PC)에 저장된 개인정보 암호화 여부	O	O	O	O
30. 개인정보처리시스템에 백신프로그램 등 최신의 보안프로그램 설치/관리 여부	O	O	O	O
31. 보안프로그램의 자동 업데이트 또는 일 1회 이상 업데이트 실시 여부	O	O	O	O
32. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 수립/운영 여부	O	O	O	O
33. 개인정보포함 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하는지 여부	O	O	O	O
34. 〈개인정보 처리방침〉에 필수항목(8개*) 포함 여부 * 8개 : 처리 목적, 처리 및 보유기간, 제3자 제공 사항(해당시), 위탁 사항(해당시), 정보주체 권리/의무 및 행사방법, 처리항목, 파기사항, 안전성 확보조치사항, 개인정보보호 책임자지정, 개인정보 처리방침의 변경이력	O	O	O	O
35. 〈개인정보 처리방침〉의 홈페이지 등 공개 여부	O	O	O	O
36. 개인정보 보호책임자 지정 여부	O	O	O	O
37. 개인정보 전담조직과 적정인력 운영 여부	X	X	O	O
38. 개인정보책임자의 교육 및 관리감독 등의 역할 수행 여부	O	O	O	O
39. 개인정보보호 예산 반영 여부	O	O	O	O
40. 개인정보 노출방지를 위한 모니터링 및 정기점검 실시 여부	O	O	O	O

발송일
2015. 11

〈대한약사회〉 주관 〈약국 자율점검 40개 체크리스트〉에서 뽑은

약국 개인정보보호 OX

본 OX는 P84의 〈약국 자율점검 40개 체크리스트〉 내용을
소만사가 재구성한 것 입니다.

안전성 확보조치
정기점검

개인정보처리시스템인 청구프로그램 DB 이외의 곳
약국 PC, 모바일, USB 등에
1. 조제기록부 등의 환자 개인정보가 복제되어 있는지
2. 고유식별정보가 방치되어있는지
   정기적으로 점검해야 합니다

약국도 개인정보 노출방지를 위한 모니터링 및 정기점검을 해야 하나요?

개인정보의 노출방지를 위해
개인정보 점검솔루션 등을 이용하여
홈페이지, PC 내 개인정보보유현황을 파악해야 합니다

O

약국 〈개인정보주체 수〉는 〈청구프로그램〉 내 환자수와 같나요?

(약국 청구프로그램 DB외
PC, 모바일, USB에
개인정보가 없다는 전제 하에)

O

약국 〈개인정보파일 수〉는 청구프로그램 조제기록부 수와 같나요?

(약국 청구프로그램 DB외
PC, 모바일, USB에
조제기록부가 없다는 전제 하에)

O

홍보,마케팅, 상담 목적으로 고유식별정보를 수집할 수 있나요?

홍보, 마케팅, 상담목적으로 개인정보를 이용할 경우 **별도 동의**를 받아야 합니다.
이 때, 고유식별정보(주민번호, 운전면허번호, 외국인등록번호, 여권번호)**는**
수집금지사항입니다

O

안전성 확보조치 정기점검 후 분리보관 및 파기

개인정보처리시스템인 청구 프로그램 DB 와
약국 PC, 모바일, USB 등에
고유식별정보, 처방전, 요양급여비용 청구처방전,
요양급여청구정보, 조제기록부 등이 있는지
점검하고 분리보관 및 파기해야 합니다

(수집목적을 달성하여 더 이상 쓰지 않을 경우) 바로 파기할 수 있나요?

(현재는 사용하지 않아도)
법령상 보유기간이 남아있을 경우
(파기 대신) 별도로 분리보관합니다

X

〈법령에 따른 보관기간〉
처방전은 2년,
요양급여 비용청구 처방전은 3년,
요양급여 청구정보는 5년,
조제기록부는 5년 보관

(법령상 보유기간이 끝나면) 법령상 보유기간이 끝나는 날짜가 다 다른데 그 날짜에 바로 파기해야 하나요?

(법령상 보유기간이 끝난) 전산데이터는
일정주기를 정하여 주기적으로
파기할 수 있습니다.
대신 위 사항을 **개인정보처리방침에 명시**해야 합니다

X

예) 소만약국 〈개인정보처리방침〉
'소만약국은 보유기간이 경과한 개인정보를
매 6개월 주기로 파기하고 있습니다'

(법령상 보유기간이 끝나면) Delete기능으로 지우기만 하면 되나요?

약국청구프로그램 DB에 있을 경우에는
약국청구프로그램에서 제공하는 파기기능을 이용합니다.
이외 PC, **모바일, USB에 있을 때는 파기솔루션**을 사용합니다

X

안전성 확보조치 정기점검 후 주민번호 암호화

개인정보처리시스템인 청구 프로그램 DB 와
약국 PC, 모바일, USB 등에
주민번호가 있는지 점검하고 암호화해야 합니다

업무용 PC or 모바일기기에 저장된 주민번호 포함파일(hwp, xls, txt)은 암호화저장해야 하나요?

네. 문서편집기의 암호설정기능이나
개인정보보호솔루션의
파일암호화기능을 활용해야합니다.

O

안전성 확보조치
제 3자 제공시 전송기록

약국 PC에서 어떤 개인정보가 언제 어디로 전송되었는지
네트워크전송, 출력, USB복제까지 기록을 남깁니다.
(제3자 관리대장의 기록으로 활용가능)

환자의 동의 없이 아래 경우 개인정보를 제공할 수 있나요?
① 처방전 접수 ② 요양급여비용 청구 ③ 약품 부작용 보고
④ 응급환자 치료를 위한 응급의료기관 요청시

법에 따라 제공가능한 경우로
고객(환자)의 동의없이 제공가능합니다

O

위 목적 이외로 환자의 동의 없이
① 의료기관 요청 ② 보험회사 요청에 따라 개인정보를 제공할 수 있나요?

고객(환자)의 동의를 받은 경우에만
제공할 수 있습니다

X

기 타

개인정보 및 개인정보처리시스템 개수

PC 2대 중 1대에만 청구프로그램이 설치되어 있습니다. 이 경우 개인정보처리시스템은 1개 인가요?

1개 입니다 O

서버에 개인정보를 저장하고 PC 5대로 접속/사용하고 있습니다. 개인정보 처리시스템은 PC개수만큼 5개로 인정되나요?

1개 입니다 X

〈개인정보보호책임자〉 및 〈개인정보취급자〉 지정

약국장만 〈개인정보보호책임자〉가 될 수 있나요?

아니오. 약국장 or 약국장이 지정한 전담직원도 〈개인정보보호책임자〉가 될 수 있습니다 X

〈개인정보보호책임자〉와 〈취급자〉를 각각 지정해야 하나요?

1인 약국은 약국장이 개인정보책임자/취급자를 겸직하며 2인 이상 약국은 분담해서 지정할 수 있습니다 X

〈개인정보보호책임자〉는 〈취급자〉에게 보안서약서를 받아야 합니까? (1인 약국은 해당사항 없음)

네. 〈개인정보보호책임자〉는 개인정보를 처리하는 근무약사, 전산직원 등 취급자에게 보안서약서를 받아 관리해야 합니다 O

〈개인정보보호책임자〉도 주기적으로 개인정보보호교육을 받아야 합니까?

네. 〈개인정보보호책임자〉는 최소 연 1회 개인정보보호교육을 받아야 합니다 O

개인정보보호교육은 〈개인정보보호책임자〉만 받아도 되나요?

아니오. 〈개인정보취급자〉도 연 1회 이상 개인정보보호 교육을 받아야 합니다. 〈개인정보보호책임자〉는 〈취급자〉들이 정기적으로 개인정보보호 교육을 받고 있는지 점검해야 합니다 X

〈개인정보보호책임자〉가 약국 내에서 다른 〈취급자〉와 함께 일반교육을 받아도 교육으로 인정해주나요?

아니오. 〈개인정보책임자〉는 전문교육 or 약사연수시 개인정보보호교육 or (www.privacy.go.kr에서) 사이버교육을 이수해야 합니다. X

위탁

약국 위탁기관에 CCTV 관리업체도 포함되나요?

네, **포함됩니다.**
그 외 위탁기관으로는 **청구프로그램업체, 처방전 보관/폐기업체**가 있습니다

O

위탁사실을 인터넷 홈페이지, 사보 등에 공개해야 하나요?

약국에서의 개인정보 처리업무 위탁사실을
(청구프로그램개발유지보수,처방전폐기, CCTV관리 등)
고객이 인지하도록 **처방접수대 등에 비치하거나 홈페이지에 공개**해야 합니다.

*필수공개사항: 위탁기관(업체)명,
위탁업무 내용, 위탁기간

O

약국도 수탁업체를 대상으로 개인정보보호교육을 진행해야 합니까?

수탁업체의 개인정보보호교육 이수 증빙서류를 받아 보관하는 것으로 교육을 대신하면 됩니다

X

위탁계약은 문서계약으로 진행해야 하나요?

네. 위탁관리에 관한 필수항목이 존재하므로
반드시 문서계약으로 진행해야 합니다

O

약국에서의 개인정보 처리업무 위탁의 예

- 처방전 보관/파기
- 약국관리프로그램 사용
  (PM2000 : 메인화면→매뉴얼→바로가기
  →개인정보처리 위탁계약서 출력)
- 약국관리프로그램 유지 · 보수(A/S)
- CCTV 위탁 관리

필수항목

- 위탁업무 수행 목적외 개인정보 처리 금지에 관한 사항
- 개인정보의 기술적 · 관리적 보호조치에 관한 사항
- 위탁하는 업무의 목적 및 범위
- 재 위탁 제한에 관한 사항
- 접근제한 등 안전조치
- 개인정보의 관리 현황 점검 등 감독에 관한 사항
- 수탁자가 준수하여야 할 의무를 위반할 경우 손해배상 등에 관한 사항

수집

조제, 복약지도시 환자 연락처를 수집할 수 있나요?

목적에 필요한
개인정보 최소수집에 해당하므로
(별도동의절차 없이)
수집할 수 있습니다

O

영상정보처리기기 설치장소에 정보주체가 인지할 수 있도록 (필수 기재사항을 포함한) 안내판을 설치해야하나요?

네, 영상정보처리기기 설치/운영시
약국 출입구 등에 고객(환자)이
인지할 수 있도록
안내판을 설치해야 합니다

X

Solution

소만사는
기술적 보호조치, 컨설팅, 개인정보 보호법규 분석 등
개인정보보호 토탈솔루션을 제공합니다

엔터프라이즈 시장1위. DB방화벽 솔루션

DB-i

- 과다조회를 이용한 불법적 유출시도 탐지
- DB접근 후 개인정보PC복제 방지기능

시장1위. WAS를 연계연동한
DB접속 기록 및 유출징후분석

was-i

- 웹접속화면 상의 개인정보 재현
- WAS를 연계연동한 DB접속자 IP/ID식별

시장1위. SAP을 연계연동한
DB접속 기록 및 유출징후분석

App-i

- SAP접속화면 상의 개인정보 재현
- SAP을 연계연동한 DB접속자 IP/ID식별
- SAP인증획득

시장 1위. 서버내 개인정보 점검 솔루션

Server-i

- DB서버, 웹서버 내 무단보관된 개인정보파일 검색
- 국내유일 CC인증 획득

시장 1위. Endpoint DLP 솔루션

Privacy-i

- PC내 개인정보 보유통제
- 개인정보포함 문서 출력시 차단, 로그기록, 원본저장

암호화웹(HTTPS)에서의 Network DLP 솔루션

Mail-i FOR Web DLP

- G메일 등 HTTPS 웹메일 , 메신저, 웹하드를 통한 개인정보 유출통제
- HTTPS Proxy와 DLP장비의 일체화
- 본문 및 첨부파일 내 개인정보패턴/개수분석

시장 1위. 세이프브라우징솔루션

WebKeeper

- 매주 5만건 이상 웹브라우징DB 업데이트
- HTTPS 접속사이트 차단
- 악성코드 차단 (좀비PC, APT/DDoS공격 예방)
- 국내유일! 리눅스 플랫폼으로 CC인증획득

시장 1위. Network DLP 솔루션

Mail-i

- 웹메일, 메신저, 웹하드를 통한 개인정보유출통제
- 〈빅데이터검색기능 〉 3년치 10억건 로그를 30초내 검색

7가지 자동화 분석툴을 통한
정교한 위험분석 방법 보유

DLP/개인정보보호에 특화된 컨설팅 서비스

- 미래창조과학부 지정 정보보안 컨설팅 전문업체
- 행정자치부 지정 개인정보 영향평가기관