SOMANSA
프라이버시레터북
2015

SOMANSA

Ⅰ. 2015 년 3대 이슈로 보는 목차

Ⅱ. 2015 년 3대 법으로 보는 목차

Ⅲ. 법 적용대상별로 보는 목차

부록. OX법률자문

Ⅰ. 2015 년 3대 이슈로 보는 목차

2015년의 보호조치 〈점검→파기〉

Ⅰ. 2015 년 3대 이슈로 보는 목차

2015년의 인물 〈CEO〉

금융기관 CEO의 위험

Ⅰ. 2015 년 3대 이슈로 보는 목차

2015년의 개인정보 〈주민번호〉

II. 2015 년 3대 법으로 보는 목차

〈개인정보보호법〉

II. 2015 년 3대 법으로 보는 목차

〈정보통신망법〉

II. 2015 년 3대 법으로 보는 목차

종합대책 기준으로 보는

〈금융기관 관련법〉

1

2011년
H사,N사 해킹사고

2011년 6월

금융위원회와 금감원 합동으로
금융회사IT보안강화종합대책 제정
주요대책으로 법규 개정 예고

웹서버는 반기, 타시스템은
연 1회 취약점 점검 등 보안강화

1차 보안강화 종합대책

2011년 10월

금융위원회
전자금융거래법고시
전자금융감독규정 개정

개인정보 PC저장금지,
사고시 업무정지 등 벌칙강화

2011년 10월

전자금융거래법, 시행령,
전자금융감독규정의
원활한 시행을 위한
권고사항으로
금융회사 IT부문
보호업무 모범규준 제정
금융권 배포

2011년 11월 14일

전자금융거래법 개정
2012년 5월 15일부터
금융기관은
CISO 의무지정

2

2013년 3월 20일
S사,N사 해킹사고

2013년 5월 22일 144p

전자금융거래법 전면개정
금융기관은 해킹으로 발생한 이용자손해에 대하여 배상할 책임을 진다

2013년 7월 11일 139p

금융보안의 패러다임을 바꾸는
금융전산보안강화종합대책 제정

2차 보안강화 종합대책

2013년 8월 1일 132p

금융기관 개인정보보호가이드라인 제정
행자부, 금융위, 금감원 합동
개인정보보호법, 신용정보보호법,
전자금융거래법 통합

2013년 11월 23일 128p

전자금융거래법 대통령령 개정시행
개인정보이용에 관한 이용자의 고의/과실 구체화
IT부문계획서 매년 3월말까지 제출
취약점 분석평가 구체화
전자적 침해행위 금지 및 침해사고 대응

3

2013년 12월
제1금융권 최초
개인정보유출사고 발생

2014년 1월
카드사
개인정보유출사고 발생

2014년 1월 13일 124p

금감원
[고객정보 유출방지를 위한 금융회사 유의사항] 발표

2014년 2월 14일 115p

금감원
금융권 3,050개사 대상 [자체점검 체크리스트] 발표

2014년 3월 10일 108p

금융분야 개인정보유출 재발방지 종합대책 발표

금융위, 금감원, 행자부, 방통위, 미래부, 기재부 범정부연합

3차 금융분야 개인정보유출 재발방지 종합대책

2014년 5월 28일 106p

금융지주회사법 개정시행
고객정보는 내부경영관리 목적으로만 제공
고객에게 고객정보 제공내역 통지

2014년 6월 30일 103p

전자금융거래법 [금융기관 검사 및
제재에 관한 규정 시행세칙] 개정시행
정보보호 소홀정도가 높을경우 기관 업무정지

2015년 4월 16일 103p

전자금융거래법
[전자금융 감독규정 시행세칙] 개정시행
외주관리 책임확대 및 구체화
보안최종책임자는 CEO임을 명시

III. 법 적용대상별로 보는 목차

관련법 개 인정보보호법 신 용정보법 정 보통신망법

01. 공통

02. 공공 · 공사 · 공단

03. 정보통신서비스 제공자

관련법 전 자금융거래법 금 융지주회사법

04. 금융

관련법 의 료법 공 공기관기록물관리법 사 회복지사업법

05. 보건복지부 산하기관

관련법 의 료법 혈 액관리법 산 업안전보건법 교 육기본법

부록. OX 법률자문

01
공통

발송일
2014. 11

개인정보보호책임자는 CEO이기에

유출사고발생/법규위반시 CEO의 리스크 [공통] 편

CEO가 대표하는 법인의 위험

1. 손해배상 소송 및 배상액 확대

2014.07.31 발표
[개인정보보호 정상화 종합대책]

- 징벌적 손해배상
- 법정 손해배상

도입

2014년
집단손해배상소송

기업측패소, 손해배상판결
(A사 1심 , B사 2심)

2. 브랜드가치 훼손

장기적, 치명적 피해

CEO 개인의 위험

3. CEO 해임가능

2014.07.31 발표
[개인정보보호 정상화 종합대책]

CEO에게 유출시
책임부과, 해임가능

2014.08.07 시행
[개인정보보호법 개정안]

법규위반시
CEO 징계권고

4. CEO 형사처벌 가능

양벌규정
(개인정보보호법 제74조)

+

2014년 이후
시대적변화

- 유출/법규위반시 **CEO** 잘못으로 판단할 가능성 상승
- **CEO,** 법인 모두 형사처벌 받을 가능성 상승

금융기관 CEO의 위험

1. 금융기관 업무정지

2014. 6. 30 실시

금감원 [금융기관검사 및 제재에 관한 규정]
시행세칙 개정안

2. 금융기관 개인정보보호 책임자로 CEO 명시

2014.03.10 발표
금감원 [금융분야 개인정보유출 재발방지종합대책]

2014.02.14 발표
금감원 [자체점검체크리스트]

2013.11.23 시행
금융위 [전자금융거래법] 개정안

2013.11.23 발표
금융위 [금융전산보안강화 종합대책]

1. 손해배상소송 및 배상액 확대!

2014.07.31 발표
개인정보보호 정상화 종합대책

고의/과실로 개인정보 유출시 앞으로 예외없는 손해배상

피해고객이 유리한 방식 선택

[징벌적손해배상]
피해자가 피해액을 입증하여 피해액의 **3배**까지 배상
개정예정 개신정

or

[법정손해배상]
피해자의 피해액 입증없이 **300만원 이내**에서 배상
개정예정 개신 11.29일시행 정

개 인정보보호법 신 용정보법 정 보통신망법

2014년 손해배상소송에서 법원이 판결한 손해배상액

2014년 8월 22일 A사 1심	1인당 10만원
2014년 2월 13일 B사 2심	1인당 100만원

2014년의 변화
[개인정보보호 정상화 종합대책]에 따라 곧 개정
개 신

2014.11.29 정보통신망법 개정 시행

고의/과실로 개인정보 유출시 손해배상금액이 회사존망을 결정지을 정도로 증가

1인당 피해액의 **3배** or 1인당 **300만원 이내**

2. 브랜드가치 훼손

[언론]
부정적인 언론보도

[임직원]
애사심저하 및 인재이탈

[고객]
소송카페 결성 및 집단소송

3. 유출사고/법규위반시 CEO 해임 의 법적근거

2014.07.31 발표
개인정보보호 정상화 종합대책

유출사고 발생시 책임자로 CEO 명시

CPO의 의무

CPO대상 **[CEO에 대한 보고의무]** 부과
위반시 과태료 **2천만원**

CEO의 책임

CEO대상 [유출시 책임] 부과, 해임 등 징계권고
시행중 **개** **신** 개정예정 **정**

개 인정보보호법 **신** 용정보법 **정** 보통신망법

2014.08.07부터 시행
개인정보보호법 개정안

법규위반시 징계대상자로 CEO 명시

개인정보보호법 제65조 (고발 및 징계권고)

② 행자부장관은 개인정보보호관련 법규위반행위가 있을 때에는 **책임있는 자(대표자 및 책임있는 임원을 포함한다)** 징계를 권고할 수 있다

사회적 분위기는
CEO 책임을
인정하는 추세

유출사고 발생시 CEO의 역할이 왜 중요한가?

바로가기

출처 : 구태언 테크앤로 대표변호사 칼럼

사고발생 후 **24시간**은 회사 존망을 가르는 **골든타임**

CEO만이 모든 부서를 아우를 수 있음

CEO만이 할 수 있는 일

신속한 〈상황실〉 설치 및 〈상황실장〉 역할수행

모든 정보가 상황실을 통해 **CEO**에게 집적되어야 함

위기상황에서 명확한 〈권한위임체계〉 수립

〈사전매뉴얼〉에 따른 명확한 권한위임체계 수립

단일한 의사결정

개인정보유출사고는 최고등급사고로 많은 의사결정 발생

예) 법적이슈, 현장조사, 언론취재, 상장기업 공시업무 등

사고발생시 **CEO**가 **간과**할 수 있는 부분 **: 통지/신고**

통지/신고를 소홀히 할 경우, 향후 손해배상소송에서 불이익 발생

정보통신망법 제 27조의3 (개인정보누출 통지 · 신고)

유출사고 발생시 **24시간이내** 이용자에게 유출사고 고지 및 **방송통신위원회 또는 한국인터넷진흥원**에 신고

24시간 이내로 고지 · 신고하지 못한 경우 방송통신위원회에 소명자료 제출

(정당한 사유없이 경과시) **과태료 3천만원**

개인정보보호법 제 34조 (개인정보 유출통지 등)

유출사고 발생시 **지체없이** 이용자에게 유출사고 고지 및 **안전행정부 또는 한국정보화진흥원, 한국인터넷진흥원**에 신고

(정당한 사유없이 경과시) **과태료 5천만원**

4. 유출사고/법규위반시 CEO 형사처벌의 법적근거

정보통신망법 제75조 (양벌규정)

② 법인의 **대표자**나 **법인의 대리인, 사용인, 종업원**이 그 법인 또는 개인의 **업무**에 관하여 71조, 72조, 74조1항, **73조의 위반행위를 하면** 행위자를 벌하는 외에 법인에게도 **벌금형**을 과(科)한다

BUT

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

71-73조 위반행위 발생시

위반 행위의 〈행위자〉 식별

직원 or 외주직원의 고의/과실이 원인일 때

2014년 이후 법의 판단은 CEO의 책임에 초점

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
직원 or 외주직원 형사처벌	법인은 벌금형

행위자처벌	법인처벌
CEO 형사처벌가능	법인은 벌금형

공통

양벌규정에 해당하는 제71-73조 위반행위 리스트

개인정보보호법 제71조 5년 이하 징역 or 5천만원 이하 벌금

- 개인정보 훼손, 멸실, 변경, 위조, 유출
- (처리할 수 없는) 고유식별정보처리
- (처리할 수 없는) 민감정보처리
- (수집할 수 없는) 개인정보수집
- 동의없이 개인정보를 제3자 제공 및 알고도 제공받은 자
- 제3자 제공이 안 되는데 제공
- 제3자 제공정보를 받고 제공범위 외로 이용
- 수탁범위 외 이용 및 제3자 제공
- 양도/합병으로 이전받고 목적 외로 이용, 제3자 제공 및 알면서 영리/부정목적으로 제공받은 자
- 업무상 개인정보를 누설, 타인제공 및 알면서 영리/부정목적으로 제공받은 자

개인정보보호법 제72조 3년 이하 징역 or 3천만원 이하 벌금

- 직무상 비밀누설 or 목적 외 이용
- 부정하게 개인정보처리에 관한 동의획득 및 알면서 영리/부정목적으로 제공받은 자
- 영상정보처리기기 임의조작,각도조절, 녹음

개인정보보호법 제73조 2년 이하 징역 or 1천만원 이하 벌금

- (정보주체의 요구에도) 개인정보를 정정/삭제하지않고 계속 이용 or 3자 제공
- (정보주체의 요구에도) 개인정보처리를 정지하지 않고 계속 이용 or 제3자제공

AND **안전성 확보조치를 하지 않은 자**

개인정보보호법 제73조 2년이하 징역 or 1천만원이하 벌금

① 다음의 **안전성 확보에 필요한 조치**를 하지 아니하여 개인정보를 분실 · 도난 · 유출 · 변조 또는 훼손당한 자

고유식별정보	영상정보처리기기	이외 개인정보
[제24조 3항] **고유식별정보** 처리시 분실 · 도난 · 유출 · 변조 또는 훼손되지 않도록 대통령령에 따라 **암호화 등 안전성 확보에 필요한 조치**를 해야 한다	[제25조 6항] **영상정보처리기기**운영자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 제29조에 따라 **안전성 확보에 필요한 조치**를 해야 한다	[제29조] 개인정보가 분실·도난·유출·변조 또는 훼손되지 않도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 **안전성 확보에 필요한 기술적·관리적 및 물리적 조치**를 해야 한다

27p [개인정보의 안전성 확보조치 기준] 규정 보기

CEO는 유출사고발생시 CEO의 형사처벌을 막기 위해
개인정보보호법고시 [개인정보의 안전성 확보조치 기준]을 모두 준수해야 한다

발송일
2014. 08

2014.07.31 발표

대한민국 개인정보보호는 적폐이자 비정상이었다

개인정보보호 [정상화 종합대책] 7대과제

원문보기 개 인정보보호법 신 용정보법 정 보통신망법

지금 무엇을 해야 하는가?

모든 기관 기업 대상

2014년 9월~12월은 국가적 [개인정보 대청소기간]

주관 : 방통위, 개인정보보호위, 인터넷진흥원, 행자부, 미래부, 금융위, 검 · 경합동수사단
협력 : 포털, 호스팅업체

〈검 · 경합동수사단〉
2014.4~2015.5
개인정보범죄 집중단속

- (상거래과정의) 불법수집, 외부무단제공, 해킹 단속
- 불법활용 단속
  신종금융사기 (대출알선/보이스피싱), 도박사이트 회원유치, 대포폰/통장

〈행자부 · 금감원〉
전국민 개인정보신고운동

〈행자부〉 국민신고센터
(☎118, privacy.kisa.or.kr)
〈금감원〉
개인정보불법유통신고센터
(☎1332, fss.or.kr)

신고& 자진삭제자 포상, 처벌감경

〈인터넷진흥원〉
웹사이트검색탐지 강화

웹사이트 개인정보 검색주기 2주→3일로 단축 ▶ 검출후 2개월 내 파기

〈한 · 중 수사협의체〉
해외불법유통 개인정보파기
(4.29 MOU체결)

〈지금 할 일〉
전사적으로 개인정보를 검출&파기 하십시오

모든 기관 기업 대상

법개정중이며 유예기간 거친후 시행

고의, 과실로 유출시 예외없는 [손해배상]

피해자가 선택

[징벌적손해배상]
피해액의 **3배**까지 배상
개정예정 개 신 정

or

[법정손해배상]
피해자의 피해액 입증없이 **300만원 이내**에서 배상
개정예정 개 신 11.29일시행 정

〈지금 할 일〉
지금 귀사의 정보유출통로를 점검하십시오

3대 [감독사각지대]+[반복적 정보유출취약지대] 명시, 구조적대책 마련

〈방통위〉 2015년 시행

통신사 대상

[개인정보 관리수준평가]
및 결과공개

통신사 · 대리점 · 영업점 대상

[의무등록제]
대리점/영업점이 통신사에 의무적등록

[전자청약시스템]으로 개인정보취득 최소화
통신사와 연결된 단말기에 개인정보입력

[SNS본인인증제]로 무단조회방지
통신사가 가입자에게 인증번호전송
→ 영업점은 인증번호로 개인정보 조회가능

[2아웃제]
대리점이 미등록판매점과 거래시 1회 영업정지 2회 아웃(=계약해지)

[5년 재등록금지]
개인정보 불법활용 영업점은 5년간 재등록금지

신용카드단말기 관리업체 대상 | **〈금융위〉 2014년 여신전문금융업법 개정예정**

[보안규정준수 카드단말기] 사용의무화
→ 위반가맹점에 벌금 500만원

텔레마케팅업체 대상 | **〈방통위〉 2014년 시행**

(개인정보사전동의없이 영업하는 TM)
수집 출처를 수신인에게 고지 의무화

[불법TM 신고]강화
- 범위확대 (통신사→전업종)
- 포상금상향 (10→20만원)

공통

정보보호산업생태계에 어떤 변화를 일으킬 것인가?

유출 사고시 책임자

CPO대상 [CEO에 대한 보고의무] 부과

→ 위반시 과태료 2천만원

CEO대상 [유출시 책임]부과, 해임 등 징계권고

시행중 개 신 개정예정 정

예산

〈미래부〉[서비스대가산정가이드라인] 발간예정

정보보호SW 업그레이드비용
도입가의 15%로 상향 (~2017년) (현재 9%)

〈미래부〉[정보보호예산편성가이드라인] 발간예정

정보화예산 중 정보보호예산비율 확대 (현재 7.3%)

[조세특례제한법] 개정예정

중소기업이 정보보호투자시 10%조세감면
(현재 7%)

〈고용부〉[고용창출지원사업]

중소기업이 정보보호인력 신규채용시
월 90만원 인건비지원

법

〈미래부〉[정보보호산업진흥법] 제정 (2014)

산업진흥을 위한 제도적 인프라구축

〈방통위〉〈금융위〉[기술적보호조치고시] 개선

[기술적보호조치]를 기업이 자율적으로
선택할 수 있도록 개선

개별법 적용대상을 명확히 하여 중복규제 해소

정보통신망법 대상 273만 → 37만 곳 신용정보보호법 대상 7만 → 3천5백 곳

개인정보보호법 적용대상

공공기관을 비롯한
모든 개인정보처리자

일반법 행자부소관

분리

신용정보보호법 적용대상

신용정보 이용/제공자
7만 곳 → 금융기관/신용정보회사
3천5백 곳

개별법 금융위소관

분리

정보통신망법 적용대상

· 정보통신망 영리사용자
(273만개 사업자 +
160만개 스마트폰앱)

→ · 전기통신/통신판매사업자
(37만개 사업자 +
160만개 스마트폰앱)

개별법 방통위소관

스마트폰, 악성코드 보안기술 강화

스마트폰 대상
[경량암호화기술]
개발(~2016)
〈미래부〉

스마트폰 출고시
[스미싱차단앱]
기본탑재 추진

[악성앱모니터링]
국내 통신사
앱마켓으로 확대
(2015)
현재 해외블랙마켓, 구글
모니터링 중

[악성코드대응체계]
모든 상용SW로
확대(~2017)
현재 웹하드업체 대상
시행중

빅데이터, 클라우드,
사물인터넷
〈개인정보보호
가이드라인〉 준비

1장으로 보는 [정상화 종합대책] 7대과제 요약

개 인정보보호법 신 용정보보호법 정 보통신망법

<table>
<tr><th colspan="2">핵심과제</th><th>상세내용</th><th>관련법 or 소관부처</th><th>기술적 보호조치</th></tr>
<tr><td>1</td><td>고의, 과실로 개인정보 유출시 [징벌적] or [법정] 손해배상</td><td>[징벌적손해배상제도] 피해액의 3배까지 배상</td><td>개정예정 개 신 정</td><td rowspan="3">[네트워크DLP] Mail-i
[엔드포인트DLP] Privacy-i</td></tr>
<tr><td></td><td></td><td>[법정손해배상제도] 피해자의 피해액 입증 없이 300만원 내에서 배상</td><td>개정예정 개 신
11.29일시행 정</td></tr>
<tr><td>2</td><td>개인정보유출은 CEO책임 명확화
〈불법취득〉〈영리목적유통〉범죄 처벌강화 + 수익몰수</td><td>CPO에게 [CEO에 대한 보고의무] 부과→위반시 과태료 2천만원
유출시 CEO책임이 있을 경우 해임 등 징계권고
<table><tr><th>범죄명</th><th>기존 최대처벌</th><th>향후 최대처벌</th></tr><tr><td>불법취득정보 영리목적제공</td><td>개 징역5년 벌금5천</td><td>개 징역10년 벌금1억</td></tr><tr><td>악성프로그램 유포자</td><td>신 징역3년 벌금3천
정 징역5년 벌금5천</td><td>신 정 징역7년 벌금7천</td></tr><tr><td>해킹범죄</td><td>신 정 징역3년 벌금3천</td><td>신 정 징역5년 벌금5억</td></tr></table></td><td>개정예정 개 신
시행중 개 신
개정예정 정
개정예정 개 신 정</td><td></td></tr>
<tr><td>3</td><td>주민번호변경 제한허용 [주민번호관리체계] 전면개편</td><td>· [주민번호관리체계] 공청회 예정 (9월)
· 주민번호수집근거법령 축소, 다른 개인식별수단 확대</td><td>[주민등록법] 개정예정</td><td></td></tr>
<tr><td>4</td><td>[개인정보대청소기간] 국가적 불법유통 개인정보 검출/파기 (2014.9월~12월)</td><td>(불법수집,외부무단제공)개인정보범죄단속
전국민 개인정보 신고운동
웹사이트검색탐지 강화
해외개인정보파기</td><td>〈검 · 경합동수사단〉
〈행자부〉〈금감원〉
〈인터넷진흥원〉
〈한 · 중수사협의체〉</td><td>[서버] Server-i
[PC] Privacy-i
[웹사이트] 개인정보검출</td></tr>
<tr><td>5</td><td>3대 [감독사각지대] 구조적 대책마련
(2014~2015)</td><td>카드단말기 관리업체 : · [보안규정준수 카드단말기] 사용의무화
· 위반가맹점에 벌금 500만원
텔레마케팅 업체 : · 개인정보 수집출처 수신인에게 고지의무화
· [불법 TM 신고] 전업종으로 확대/포상금 상향(10→20만원)
통신사 (대리점 /영업점) : · [개인정보관리수준평가] / 결과공개
· [의무등록제] [전자청약시스템] [SNS본인인증]
· [투아웃제] [5년 재등록금지]</td><td>〈금융위〉 [여신전문금융업법] 개정예정
〈방통위〉
〈방통위〉</td><td></td></tr>
<tr><td>6</td><td>자율적투자, 예방여건 조성</td><td>· 정보보호SW 업그레이드비용 도입가의 15%로 상향 (~2017)
· 정보화예산 중 정보보호예산비율 확대
· 중소기업이 정보보호투자시 2017년까지 조세감면 확대 (10%)
· 중소기업이 정보보호인력 채용시 월 90만원 지원
· 스마트폰, 악성코드보안기술강화
· 빅데이터,클라우드,사물인터넷 〈개인정보보호가이드라인〉마련</td><td>〈미래부〉</td><td>[악성코드] 세이프브라우징 WebKeeper
[스마트폰] SMART-i</td></tr>
<tr><td>7</td><td>법 적용대상 명확화 중복규제 해소</td><td><table><tr><th>법</th><th>기존 적용대상</th><th>향후 적용대상</th><th>소관부처</th></tr><tr><td>개</td><td>· 공공기관을 비롯 모든 개인정보처리자</td><td>· 공공기관을 비롯 모든 개인정보처리자
* 개별법적용대상은 각 소관부처에 위임위탁</td><td>행자부</td></tr><tr><td>신</td><td>· 신용정보이용/제공자 7만곳</td><td>· 금융기관/신용정보회사 3천5백곳</td><td>금융위</td></tr><tr><td>정</td><td>· 정보통신망을 영리로 사용하는자 사업자 273만곳+스마트폰앱 160만개</td><td>· 전기통신사업자/통신판매사업자 사업자 37만곳 +스마트폰앱 160만개</td><td>방통위</td></tr></table></td><td></td><td></td></tr>
</table>

공통

발송일
2014. 07

2014년 8월 7일 개정 개인정보보호법 시행! [주민번호수집금지제도가이드라인] 분석 ②

주민번호 수집·이용! 어떨 때 가능 VS 불가능 한가?

원문보기

O 주민번호수집가능 X 주민번호수집불가능

주민등록증 확인 후 적거나 보관하지 않고 바로 돌려주는 것은 주민번호수집이 아님

주민번호 앞 6자리는 생년월일 정보로 주민번호가 아님

주민번호 뒤 7자리는 고유한 식별정보로 주민번호에 해당

금융/보험/세금 관련업무는 대부분 가능

O 계좌개설, 급여지급 등 금융거래업무

금융실명거래 및 비밀보장에 관한 법률 제3조
금융회사는 거래자 실지명의로 금융거래를 해야 한다
*실지명의 : 주민등록상의 명의를 의미(동법 2조)

O 현금영수증

조세특례제한법 제126조의3 5항
국세청장은 소득공제 등 현금영수증제도운영을 위해 성명, 주민번호 등을 요청할 수 있다

O 연말정산 관련문서

소득세법 시행령 제108조
배우자, 부양가족유무 확인은
주민등록표등본, 가족관계등록부 증명서에 의한다

O 원천징수영수증

소득세법 시행규칙 제100조 25호
원천징수영수증, 지급명세서에 주민번호 기재 명시

O 사회적배려대상자 공공요금 절감

법령개정 중
가스, 전기, 수도요금감면 대상자 신원확인,
부정수급방지를 위해 주민번호가 필요함을 인정

O 콜센터 금융거래관련 상담

금융실명거래 및 비밀보장에 관한 법률 제3조
에 따라 금융거래 상담시 주민번호수집가능
콜센터 일반상담시 주민번호 수집이용 불가능

O 임직원 단체보험가입

보험업법 시행령 제102조 5항
보험회사는 보험체결, 보험금지급 등을 위해 주민번호, 여권번호, 운전면허번호, 외국인등록번호 포함자료를 처리할 수 있다
- 회사는 보험회사를 대신해 임직원 주민번호를 수집, 보험회사에 보낼 수 있음
- 보험가입만을 위하여 신규수집한 주민번호는 전달 후 즉시 파기해야함

X 보험증권 상 주민번호 기입

보험업법 내
보험증권에 대한 주민번호 수집이용 규정없음
*보험증권 : 보험계약성립을 증명하는 문서

인사/총무 관련업무

O 직원신규채용 (입사확정)

국민건강보험법, 근로기준법, 소득세법에 따라 가능

X 이력서 (입사미확정)

행자부 인사/노무분야 개인정보보호 가이드라인 21P
고유식별정보(주민번호 등), 민감정보(종교, 정치성향 등) 수집 · 이용은 원칙적으로 금지

O 근로자 퇴직후 주민번호 보관

근로기준법 제39조 1항
에 따라 재직증명서, 근로소득증명, 보험연계처리를 위해 3년간 보관 가능
*3년 이상 보관필요성을 인정하여 근로기준법 3년 보관규정 개정 예정

X 사내증명서

명시적 주민번호 사용규정이 없음

X 사내주차증, 차량출입증 발급

행자부 주민번호 수집금지제도 가이드라인 19P
대체수단을 도입하거나
차량등록증이나 운전면허증 확인후 반환하거나
차량등록증 내 주민번호항목을 삭제한 사본 접수

X 기업 사옥 출입증 교부

행자부 주민번호 수집금지제도 가이드라인 17P
생년월일, 연락처정보로 대체
주민등록증을 육안으로 확인하고 돌려주는 행위는 주민번호처리가 아니므로 가능

의료

O 진단서, 처방전, 진료기록부

의료법 시행규칙 제9 · 12 · 14조
진단서, 처방전, 진료기록부에는 환자의 이름 · 주소 · 주민번호를 기록해야 한다

X 임직원건강검진목적으로 회사가 주민번호를 수집해서 병원으로 전달

산업안전보건법, 의료법 내 건강검진을 위해 주민번호를 수집하라는 규정 없음

O 임직원 건강검진을 의뢰받은 병원에서 임직원 주민번호를 수집(건강진단결과 회신목적)

근로자 건강진단 실시기준 제13조
병원이 건강진단을 실시했을 때 그 결과를 건강진단개인표(주민번호 포함)에 기록하고 근로자에게 보내야 한다

O 진료예약 (내원, 인터넷, 전화)

의료기관 개인정보보호 가이드라인 6P
수집정보
주민번호, 성명, 주소, 연락처, 진료과목

2015.02 의료기관 가이드라인 개정내용
전화와 인터넷 등을 이용한 진료/검사예약시
건강보험가입/건강검진대상여부 확인이 필요한 경우 주민번호 수집가능

소송 및 신고접수

O 법원소송 관련서류

법원에 소송을 제기하는 자의
주민번호처리에 대한 법령이 없어서 법령개정중
소송의 경우 특정인을 명확히 할 필요가 있으므로
소송서류에 주민번호 수집가능

X 정보통신망법에 따른 (기업대상) 권리침해신고접수

정보통신망법 제44조의 2 1항에 따라
정보통신망에 사생활침해정보가 올라갔을 경우
정보통신서비스제공자에게 신고할 수 있다
이때 대면신고시 신분증,
비대면신고시 주민번호대체수단을 활용한다

본인확인 및 계약은 대부분 불가능

X 멤버쉽회원 본인확인(마트, 백화점)

행자부 주민번호 수집금지제도 가이드라인 16P
아이핀, 생년월일+휴대폰번호 조합 등
주민번호 대체수단 활용

X 콜센터상담시 본인확인절차

행자부 주민번호 수집금지제도 가이드라인 33P
생년월일, 휴대폰, 거래내역으로 본인확인가능

X 홈페이지 회원가입

행자부 주민번호 수집금지제도 가이드라인 14P
아이핀, 생년월일+휴대폰번호 조합 등
주민번호 대체수단 활용

X 아이디/비밀번호 분실시 본인확인절차

행자부 주민번호 수집금지제도 가이드라인 35P
아이핀, 휴대폰인증 등 대체수단을 통해
아이디 · 비밀번호 확인가능

X 렌터카 계약시

행자부 주민번호 수집금지제도 가이드라인 16P
운전면허번호로 대체
렌터카보험 가입시 보험업법에 근거하여 주민번호 수집가능

X 고속버스 예약시 주민번호수집

행자부 주민번호 수집금지제도 가이드라인 19P
주민번호 삭제 / 필요시 대체수단 도입
신용카드로도 신원확인 가능

X 표준약관에 따른 주민번호처리

행자부 주민번호 수집금지제도 가이드라인 17P
조직이 자체적으로 정한 표준약관에 따라 수집할 경우 법령근거가 있나를 먼저 확인해야 하며
표준약관에서 정했다고 해서 수집할 수는 없음

발송일
2014. 07

2014년 8월 7일 개정 개인정보보호법 시행! [주민번호수집금지제도가이드라인] 분석 ①

모든 공공·민간사업자 주민번호 수집·이용금지 위반시 과태료 3,000만원

원문보기

2014년 8월 7일 부터 무엇이 달라지는가?

주민번호 수집 · 이용시 3천만원 과태료	이미 보유한 주민번호 2016.8.7까지 파기	주민번호 유출시 과징금 5억	개인정보보호법 위반시 대표이사 · 임원 징계

근거법령이 있는 경우 수집 · 이용가능

주민번호 수집 · 이용 허용사유

개인정보보호법 제24조의2 (주민번호처리의 제한)

① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민번호를 처리할 수 없다.

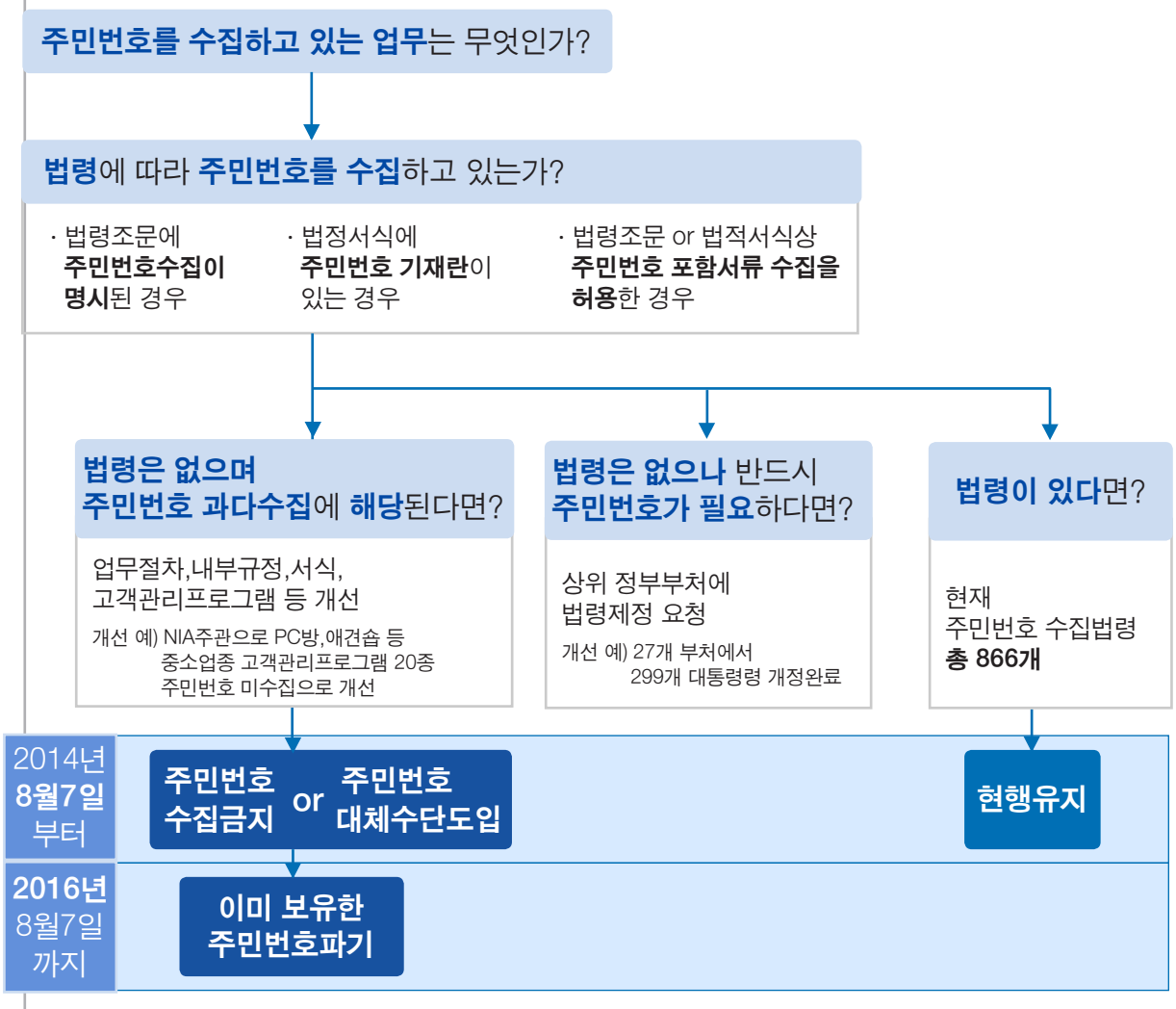
1. **법령**에서 구체적으로 주민번호처리를 요구 · 허용한 경우
2. 정보주체 or **제3자의 급박한 생명,신체,재산의 이익을 위해** 명백히 필요한 경우
3. 기타 주민번호처리가 불가피한 경우로서 **행정자치부령**으로 정하는 경우

행자부·방통위·금융위 합동 주민번호 수집 · 이용금지 어떻게 진행되어왔나?

- 2012.04.24 행자부 · 방통위 · 금융위 **[주민번호 수집 · 이용 최소화 종합대책]**
- 2012.08.18 방통위 **정보통신망법 개정시행 주민번호 수집 · 이용금지**
- 2013.08.07 행자부 **개인정보보호법 개정공포**
- **2014.08.07 행자부 개인정보보호법 개정시행 주민번호 수집 · 이용금지**
- **2014.08.17까지 방통위 정보통신망법에 따라 기보유 주민번호 파기**
- 2016.08.07까지 행자부 **개인정보보호법에 따라 기보유 주민번호 파기**

주민번호, 어떨 때 파기하고 어떨 때 저장하는가?

전사적 주민번호 검출/현황분석 아직 안하셨다면 지금 하셔야 합니다



발송일
2014. 07

2014년 12월 30일 개인정보보호법고시

[개인정보의 안전성 확보조치 기준] 개정시행

2011년 9월(고시 제43호) 이후 최초의 대대적 개정
무엇이 바뀌나?

개 정 방 향	신 설 규 정		
2014년 1월 발생 **카드사 유출사고 재발방지**	3조 ①항 [내부관리계획]에 [개인정보처리업무 수탁 경우 수탁자 관리감독] 포함	7조 ②항 개인정보처리시스템 접속기록 반기별로 1회 이상 점검	9조 ③항 개인정보포함 보조저장매체의 반출입 통제대책 마련
개인정보 파기규정 대통령령에 있던 파기규정을 세분화, 현실화하여 명시	10조 ①항 개인정보 파기시 1. 완전파괴(소각, 파쇄 등) 2. 전용소자장비로 삭제 3. 포맷 or 덮어쓰기	10조 ②항 개인정보 일부파기로 ①항이 어려울 경우 1. 전자적파일 개인정보 삭제후 복구/재생되지 않도록 관리 2. 기록물(인쇄물,서면,기록매체) 해당부분 마스킹 or 천공	
모바일기기를 업무용 컴퓨터 수준으로 격상 **개인정보보호 의무화**	5조 ④항 개인정보가 홈페이지, P2P, 공유설정, 공개된 무선망 등을 통해 공개 · 유출되지 않도록 모바일기기에 조치	5조 ⑦항 분실 · 도난으로 인한 개인정보 유출을 대비하여 모바일기기에 비밀번호설정	6조 ⑦항 모바일 기기에 고유식별정보 저장시 상용암호화SW or 안전한 암호화 알고리즘으로 암호화
인터넷 홈페이지 보안강화	5조 ③항 홈페이지에서 성명 · 주민번호로 본인인증시 추가인증수단 제공	5조 ⑤항 고유식별정보 유출 · 변조 · 훼손방지를 위해 연 1회 이상 홈페이지 취약점 점검	
방지 · 치료해야 하는 **악성프로그램 구체화**	8조 키보드 · 화면 · 메모리탈취 등 신종변종을 포함한 악성프로그램 등을 방지 · 치료할 수 있는 보안프로그램 설치 · 운영		

[고시]에 개정되지는 않았으나 상위법개정(2014년 개인정보보호법률개정)에 따른 변화는?

상위법에 따른 변화 1 개인정보처리시스템에 〈DB연동 · 연계 어플리케이션〉 포함

2014년 3월 24일부터 시행

개인정보보호법 제2조 2호

개인정보처리의 범위확장

개인정보의 수집,생성,기록,저장,보유,가공 편집,검색,출력,정정(訂正),복구,이용,제공, 공개,파기(破棄) ＋**연계,연동**

어플리케이션(WAS,SAP 외) 등 DB와 연계, 연동된 시스템도 개인정보처리시스템에 명시적으로 포함

WAS, SAP에 보호조치의무화

4조	5조	7조
접근권한 관리	접근통제	접속의 보관 및 점검

상위법에 따른 변화 2 2016년 1월 1일까지 [고시] 6조 ⑤항 개정예정

현재

영향평가 혹은 위험도분석 **결과에 따라** 내부망 주민번호 암호화

6조 ⑤항
내부망에 고유식별번호 저장시
암호화적용여부 및 범위는 다음 기준에 따른다
1. (공공기관 경우) 영향평가 결과
2. (기업체 경우) 위험도분석 결과

2016년 1월 1일부터 시행

주민번호는 영향평가 혹은 위험도분석 **결과에 상관없이** 내부망 저장시에도 암호화

이전 Report 보기

[개인정보의 안전성 확보조치 기준] 고시 상세규정보기

조	내용	기존과 달라진 점	관리적 보호조치
1조 목적	(법 24조3항 · 29조, 시행령 21 · 30조에 따라) 개인정보가 분실,도난,유출,변조,훼손되지 않도록 (개인정보처리자가 지켜야하는) 안전성확보기준을 정함		
2조 정의	〈총 18개의 용어정의〉 정보주체, 개인정보파일, 개인정보처리자, 소상공인, 중소사업자, 개인정보보호책임자, 개인정보취급자, 정보통신망, **개인정보처리시스템**, 내부망, 내부관리계획, 비밀번호, 접속기록, 바이오정보, 보조저장매체, 위험도분석 **모바일기기** (→무선망을 통해 개인정보처리에 이용되는 휴대기기 ex, PDA, 스마트폰, 태블릿PC 등) **공개된 무선망** (→불특정다수가 무선접속장치(AP)를 통해 인터넷을 이용할 수 있는 망)	삭제 P2P, 공유설정 **신설** 모바일기기, 공개된 무선망	**상위법에 따른 변화1** 개인정보 처리시스템에 WAS, SAP 등 어플리케이션이 포함되므로 보호조치 필요
3조 내부관리 계획의 수립 · 시행	① 내부관리계획에 포함되는 사항 1. 개인정보보호책임자지정 2. 개인정보보호책임자 및 취급자의 역할 · 책임 3. 개인정보의 안전성 확보에 필요한 조치사항 4. 개인정보취급자교육 **5. 개인정보처리업무 위탁시 수탁자관리감독** 6. 그 밖에 필요한 사항	**신설** 5. 위수탁자관리감독	Privacy consulting
	② 소상공인은 내부관리계획을 수립하지 않아도 됨		
	③ 1항에 변화가 생길시, 즉시 수정 및 시행 후 이력관리		
4조 접근권한의 관리	① 업무필요 최소한의 범위로 접근권한 차등부여		
	② 인사이동시 접근권한 변경 또는 말소		
	③ 권한 부여 및 변경내역 최소 3년간 보관		
	④ 취급자별 한 개의 계정사용, 계정공유금지		
	⑤ (개인정보취급자 또는 정보주체대상) 비밀번호 작성규칙수립 및 적용	**변경** 기존 5조 비밀번호관리를 4조 ⑤항으로 변경	

(뒷장에서 계속)

[개인정보의 안전성 확보조치 기준] 고시 상세규정보기 (앞장에서 계속)

조	내용	기존과 달라진 점	기술적 보호조치
5조 접근통제	① 불법접근, 침해방지를 위해 다음기능 포함조치 1. 개인정보처리시스템접속권한을 IP등으로 제한하여 인가받지 않은 접근 제한 2. 개인정보처리시스템 접속 IP등을 분석, 불법유출시도 탐지	변경 다음기능을 포함한 시스템 → 다음기능포함조치	[DB방화벽(접근통제)] DB-i
	② 취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속할 경우 VPN 또는 전용선 등 안전한 접속수단 적용		
	③ 인터넷홈페이지에서 다른 법령에 근거하여 성명, 주민번호를 이용하여 본인을 확인하는 경우 추가인증수단제공	신설	
	④ 개인정보가 홈페이지, P2P, 공유설정, **공개된무선망** 등을 통해 공개, 유출되지 않도록 개인정보처리시스템, 컴퓨터, **모바일기기**에 조치	추가 모바일기기, 공개된 무선망	[Network DLP] Mail-i™ [Endpoint DLP] Privacy-i
	⑤ 인터넷홈페이지에서 고유식별정보가 유출, 변조, 훼손되지 않도록 연 1회 이상 취약점 점검	신설	[웹사이트 개인정보검출] 웹프라이버시
	⑥ 업무용컴퓨터 또는 **모바일기기**를 이용하여 개인정보를 처리할 경우 1항을 적용하지 않을 수 있으며 이 경우 OS나 보안프로그램 등에서 제공하는 접근통제기능을 사용한다	추가 모바일기기 번호변경 기존 ⑧항을 ⑥항으로 변경	[모바일기기내 개인정보검출 및 파기 · 암호화] SMART-i
	⑦ 개인정보처리에 이용되는 모바일기기의 분실, 도난으로 개인정보가 유출, 변조, 훼손되지 않도록 모바일기기에 비밀번호설정을 해야 한다	신설	
6조 개인정보의 암호화	① (시행령 제21조 및 제30조 1항 3호에 따라) 고유식별정보 (주민번호, 여권번호, 운전면허번호, 외국인번호), 비밀번호, 바이오정보 암호화		[DB] DB암호화 [PC] Privacy-i DRM
	② (고유식별정보, 비밀번호, 바이오정보를) 정보통신망으로 송수신, 보조저장매체로 전달시 암호화		보안서버(SSL 외) [DB] DB-i [보조저장매체] Privacy-i
	③ 비밀번호 및 바이오정보는 암호화저장 해야하며 비밀번호는 복호화되지 않도록 일방향 암호화한다		
	④ 인터넷구간 및 인터넷과 내부망의 중간지점 (DMZ : Demilitarized Zone)에 고유식별정보 저장시 암호화		[서버] Server-i
	⑤ 내부망에 고유식별정보 저장시 암호화 적용여부 및 범위는 다음 기준에 따른다 1. (법 제33조에따라) 영향평가결과 영향평가대상 공공기관 경우 2. 위험도분석 결과		상위법에 따른 변화2 개인정보보호법 24조의2 ②항에 따라 2016.01.01까지 개정예상
	⑥ (고유식별정보, 비밀번호, 바이오정보를) 암호화 할 경우 안전한 암호알고리즘으로 암호화하여 저장		DRM [DB] DB암호화 [PC] Privacy-i
	⑦ 업무용 컴퓨터 또는 **모바일기기**에 고유식별정보저장시 상용암호화SW 또는 안전한 암호화 알고리즘으로 암호화저장	추가 모바일기기	[PC] Privacy-i [모바일] SMART-i

(뒷장에서 계속)

[개인정보의 안전성 확보조치 기준] 고시 상세규정보기 (앞장에서 계속)

조	내용	기존과 달라진 점	기술적 보호조치
7조 접속기록의 보관 및 점검 기존명칭 접속기록의 위변조보관 및 방지	① 개인정보처리시스템 접속기록 최소 6개월이상 보관 · 관리		[DB] DB-i [WAS] was-i [SAP] App-i
	② 개인정보처리시스템 접속기록 반기별로 1회 이상 점검	**신설**	
	③ 접속기록이 위 · 변조 및 도난, 분실되지 않도록 해당접속기록을 안전하게 보관		
8조 악성 프로그램 등 방지 기존명칭 접근통제 시스템 설치 및 운영	**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	**추가** 악성프로그램 구체화	[방지] 세이프브라우징 솔루션 WebKeeper™ [치료] · 백신
9조 물리적 접근방지	① 물리적 개인정보 보관장소 출입통제절차 수립 · 운영		Privacy-i 개인정보가 보조저장매체, 서류로 복제되는 것을 최소화함으로써 물리접근방지대상 최소화효과
	② 개인정보 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관		
	③ 개인정보포함 보조저장매체의 반출입통제를 위한 보안대책 마련		
10조 파기	**① 개인정보 파기시 다음 중 하나의 조치를 해야 한다** **1. 완전파괴 (소각, 파쇄 등)** **2. 전용소자장비를 이용하여 삭제** **3. 데이터가 복원되지 않도록 포맷 or 덮어쓰기 수행**	**신설**	Privacy-i 복구 불가능하도록 7회이상 파기
	② 개인정보의 일부만을 파기할 때에는 제 ①항의 방법으로 파기하는 것이 어려운 경우 다음 각 호의 조치를 하여야 한다 **1. 전자적 파일 형태인 경우 개인정보를 삭제한 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**		

발송일
2014. 03

2014 개인정보보호법 개정

변화 1 어플리케이션(WAS, SAP) 연계, 연동시스템까지 <개인정보처리시스템>으로 범위확대

변화 2 주민번호는 내부망저장시에도 암호화

개보법일부개정안 원문보기

변화 1 〈개인정보처리시스템〉의 범위를 애플리케이션까지 확장

개인정보보호법 제2조 2호

〈개인정보처리시스템〉 의 범위확장

개인정보의 수집, 생성, 기록, 저장, 보유,
가공, 편집, 검색, 출력, 정정(訂正), 복구,
이용, 제공, 공개, 파기(破棄)

+ 연계/연동

개정 2014년 3월 24일부터 시행

개인정보보호법 제2조 2호

애플리케이션(WAS,SAP 외)시스템 등
DB와 연계, 연동된 개인정보시스템도
〈개인정보처리시스템〉 에 명시적으로 포함

(기존에도 사실상 포함으로 해석)

따라서

WAS, SAP 에 개인정보보호법고시
[개인정보의 안전성 확보조치 기준] 조치해야 함

- 접속기록 저장
- 접근통제
- 반기별 1회 점검

변화 2 주민번호는 내부망 저장시에도 암호화

이전

영향평가 or 위험도분석 결과에 따라
내부망 주민번호 암호화

개인정보보호법고시
'개인정보의 안전성 확보조치 기준' 제7조 5항

내부망에 고유식별번호 저장시
암호화적용여부/범위는 다음 기준에 따른다
1. (공공기관 경우) 영향평가 결과
2. (기업체 경우) 위험도분석 결과

신설 2016년 1월 1일부터 시행

주민번호는
영향평가 or 위험도분석 결과에 상관없이
내부망에 저장될시에도 암호화

개인정보보호법 제24조의2 2항

② 개인정보처리자는 제24조제3항에도 불구하고 주민번호가 분실/도난/유출/변조 or 훼손되지 아니하도록 암호화조치를 통하여 안전하게 보관하여야 한다.
이 경우 암호화적용대상/대상별 적용시기등에 관하여 필요한 사항은 개인정보의 처리규모와 유출시 영향 등을 고려하여 대통령령으로 정한다.

발송일
2013. 11

개인정보보호법에 따른

공공기관/기업대상 PIPL(개인정보보호수준 인증제) 시행

(PIPL : Privacy Information Protection Level)

원문보기

· 개인정보보호법 [개인정보보호수준 인증제] 란?
행자부가 공공기관과 기업의 **개인정보보호수준을 점검해 인증마크를 부여**하는 제도

[개인정보보호 인증마크]

· 인증을 실제 수행하는 기관은 어디인가? NIA 한국정보화진흥원

· 누가 신청할 수 있는가?
공공기관과 기업(기업 경우 **대기업, 중소기업, 소상공인**별로 심사기준 차등화)

· 인증대상범위는 어떻게 되는가?
기관이나 기업 **전체도 가능 or 특정서비스**에 한정하여 신청가능

· 인증절차는
〈1차〉 **서면심사** (〈개인정보처리시스템〉 목록, 개인정보보호관리체계 수립운영방법 절차 및 관리체계, 보호대책 구현과 관련되는 문서목록 제출)
〈2차〉 **현장심사**로 진행

· 유효기간은? 인증마크 발급일로부터 **3년**간 유효

인증마크를 획득하면 어떤 혜택이 있는가?

개인정보보호법고시 [개인정보보호수준 인증제 운영에 관한 규정] 제28조(인증취득기관의 혜택)

혜택1
행정자치부장관은 인증취득기관에게 [개인정보보호법]에 따라
실시하는 기획점검 대상 제외 or 실시유예,
행정처분 감경등의 혜택을 줄 수 있다

혜택2
개인정보보호우수기관**포상,**
개인정보보호수준인증 **관련 교육,**
행사참여기회 등의 혜택을 제공할 수 있다

(개인정보보호 관련 기존 유일인증이었던) PIMS인증과의 차이

〈PIMS인증〉
· 정보통신망법 시행기관인
방통위, 한국인터넷진흥원(KISA)이 주관
· 정보통신서비스제공기업 대상 인증
· 2011년부터 시행

VS

〈PIPL인증〉
· 개인정보보호법 시행기관인
행자부, 한국정보화진흥원(NIA)이 주관
· 공공기관, 대기업, 중소기업, 소상공인 대상 인증
· 2013년 11월 28일 부터 시행

PIPL 인증 심사기준

인증유형	심사항목 (개)		
	개인정보보호 관리체계 (15항목)	개인정보 보호대책구현 (50항목)	합계
대기업/공공기관	15	50	65
중소기업	8	44	52
소상공인	0	33	33

대기업/공공기관은 심사항목을 100% 준수해야 함

PIPL인증 심사기준상의 기술적 보호조치

보호관리과정

심사 항목	심사내용	인증심사시 점검항목	적용대상				기술적 보호조치
			공공 기관	대 기업	중소 기업	소상 공인	
2.2.1 식별	개인정보자산식별 / 목록생성, 관리	· 개인정보자산을 식별하는가? · 자산목록을 지속관리하는가? · 책임소재가 명확한가? · 개인정보자산을 중요도에 따라분류하는가?	O	O	O		·Privacy-i로 PC내 자산식별 / 분류 ·Server-i로 DB / 서버내 자산식별

보호대책구현

심사 항목	심사내용	인증심사시 점검항목	적용대상				기술적 보호조치
			공공 기관	대 기업	중소 기업	소상 공인	
5.3.2 파일 관리	개인정보 파일현황을 행자부에 등록	(기관장이 행자부장관에게) · 개인정보파일등록 or 변경사항고지 여부	O	O	O		·Privacy-i로 PC내 자산식별 / 분류 ·Server-i로 DB / 서버내 자산식별
5.4.2 파기	파기계획에 따라 안전한 방법으로 지체없이 파기	· 목적달성시 지체없이 복구할 수 없게 파기하는가? · 타법령에 근거하여 보유시 별도분리하는가?	O	O	O		·Privacy-i로 PC내 개인정보파기 ·Server-i로 서버내 개인정보파기 · 파일삭제솔루션 · 디가우저 · 문서파기솔루션(슈레더)

(뒷장에서 계속)

보호대책구현 (앞장에서 계속)

심사 항목	심사내용	인증심사시 점검항목	적용대상				기술적 보호조치
			공공 기관	대 기업	중소 기업	소상 공인	
8.1.2 권한 관리	〈개인정보처리시스템〉 접근권한 최소부여	· 접근권한을 최소한의 범위로 차등부여하는가? · 퇴직/직무변경시 접근권한이 제거되는가? · 권한부여, 변경, 말소내역을 최소 3년간 보관하는가? · 한 계정으로 다수가 동시접속 할 수 없도록 조치했는가?	O	O	O	O	· DB방화벽 DB-i의 접근통제기능 (1인 1계정 부여기능외) · WAS를 통한 최종 조회자 추적 솔루션 was-i의 접근통제기능
8.1.3 접근 권한 검토	〈개인정보처리시스템〉 접근권한정기점검	· 접근권한을 주기적으로 검토하는가? · 특수접근권한을 제한하고 주기적으로 점검하는가? · 권한검토결과에 따라 조치하는가?	O	O	O		
8.2.1 접속 기록 관리	〈개인정보처리시스템〉 접속기록보관/보호	· 접속기록을 위/변조방지 보관하는가? · 접속기록을 최소 6개월 이상 보관/관리하는가?	O	O	O	O	· DB-i, was-i의 로그위변조방지기능 · WORM스토리지, CD, DVD
8.2.2 접속 기록 검토	〈개인정보처리시스템〉 열람/처리기록 주기적 분석	· 개인정보취급자의 접속기록을 분석하고 주기적으로 검토하는가?	O	O	O		· DB방화벽 DB-i의 접속기록보관 / 이상징후검색기능 · WAS를 통한 최종 조회자 추적 솔루션 was-i의 접속기록 보관 / 이상징후검색기능
8.3.3 개인 정보 처리 보호 조치 활동	〈개인정보처리시스템〉 비인가접근시도 모니터링	· 비인가접근시도 , 허가된 접근을 모니터링하는가?	O	O	O		
8.3.4 개인 정보 표시 제한	개인정보조회, 출력시 마스킹	· 조회/출력시 마스킹기준을 정하고 시행하는가?	O	O	O		· DB방화벽 DB-i의 화면조회시 개인정보마스킹

(뒷장에서 계속)

보호대책구현 (앞장에서 계속)

심사 항목	심사내용	인증심사시 점검항목	적용대상				기술적 보호조치
			공공 기관	대 기업	중소 기업	소상 공인	
8.3.5 접근 통제 시스템 설치 운용	정보통신망을 통한 불법접근/ 침해방지를 위해 침입차단/방지기능 설치운용	· 침입차단/침입방지기능을 운영하는가? · 허가된 사용자 PC/IP에서만 접근가능하도록 접근통제를 하는가?	O	O	O	O	· DB방화벽 DB-i 의 접근차단 / 접근통제기능 · 방화벽 / IPS
8.3.6 네트 워크 접근 통제	입법예고 이후 추가항목 네트워크분리 등 기술적보호조치 마련	· 웹서버 앞단에 웹해킹예방/ 공격탐지,제거를 위한 웹방화벽을 설치하고 있는가?	O	O			· 웹 방화벽
8.3.7 네트 워크 운영 관리	〈개인정보처리 시스템〉 접속시 접근제한 / 보호	· 〈개인정보처리시스템〉에 특정 단말만 접근할 수 있도록 접근제한하고있는가? · 외부 네트워크를 통한 접속시 VPN or 전용선 등 안전한 접속수단을 적용하는가?	O	O	O		· DB방화벽 DB-i 의 전송시 암호화기능 (DB VPN) · 일반 VPN
8.8.2 암호화	개인정보 저장/전송/ 원격접속시 암호화	· 인터넷구간, DMZ에 고유식별 정보, 민감정보, 비밀번호를 암호화저장하는가? · 내부망저장시 위험도분석 등을 통해 암호화 or 상응되는 조치를 하는가? · PC에 고유식별정보, 민감정보, 비밀번호를 암호화저장하는가? · 개인정보를 정보통신망 및 보조 저장매체로 전달시 고유식별 정보,민감정보, 비밀번호를 암호화하는가? · 원격으로 내부시스템접근시, VPN등으로 암호화통신하는가? · 안전한 암호화 알고리즘을 사용하는가?	O	O	O	O	· Privacy-i 로 PC / 보조저장매체내 개인정보암호화 · DB-i 로 정보통신망 전송시 암호화 · Server-i 로 DMZ구간내 서버저장시 암호화 · 국정원인증 알고리즘 사용 · DRM · PC 보안솔루션 · DB암호화

삭제

발송일
2013. 10

2014.08.07부터 시행

2013 [개인정보보호법] 개정 요약

1. 2014.08.07부터 주민번호수집금지
2. 주민번호유출시 과징금 5억
3. 법규위반시 대표이사 징계

정보주체가 동의하더라도

2014년 8월 7일부터 **주민번호 수집·이용금지** 위반시 3천만원 이하 과태료 부과

2016년 8월 7일까지 **보유한 주민번호파기**

[개인정보의 안전성 확보조치 기준]을 하나라도 준수하지 않아서

주민번호유출시 과징금 최대5억

개인정보보호 법규위반시 대표자/임원 징계

2013년 개인정보보호법 개정! 무엇이 달라지나? 원문보기

개인정보보호법 개정안 변화 1

기존

①~~정보주체의 동의가 있는 경우~~
②법령에 근거가 있는 경우
주민번호 수집 · 이용가능

신설 제24조의2 (주민번호의 처리제한)

①다음 경우에만 주민번호 수집, 이용가능
1. 법령에 구체적인 근거가 있는 경우
2. 급박한 생명, 신체,재산상 이익을 위해 명백히 필요한 경우
3. 행자부령으로 정하는 경우

정보통신망법 개정에 따라
온라인상 주민번호 수집금지는
현재 시행중(2013년 2월18일부터 시행)

(2014년 8월부터)
개인정보보호법 개정에 따라
온라인/오프라인 모두
주민번호 수집금지

공통

개인정보보호법 개정안 변화 2

기존

주민번호 분실·도난·유출·변조·훼손시 과태료, 형사처벌

신설 제34조의2 (과징금의 부과 등)

① 주민번호 분실·도난·유출·변조·훼손시
(과태료, 형사처벌 외) 5억원 이하의 과징금을 부과 · 징수할 수 있다
다만, 안전성 확보에 필요한 조치를
모두 준수한 경우에는 그러하지 아니하다

개인정보보호법 개정안 변화 3

기존

행자부장관은
개인정보보호관련 법규위반행위가
있을 때에는 책임있는 자 징계를
권고할 수 있다

개정 제65조 2항 (고발 / 징계권고)

행자부장관은
개인정보보호관련 법규위반행위가 있을 때에는
책임있는 자(대표자 / 책임있는 임원) 징계를 권고할 수 있다

징계권고대상 명확화
책임 있는 자 = 대표자, 책임있는 임원

'CEO, CISO, CIO'
보안책임강화

27p [개인정보의 안전성 확보조치 기준] 규정 보기

유출사고 발생시 처벌을 피하고, 법규위반으로 인한 대표자 , 임원징계를 막기 위해
개인정보보호법고시 [개인정보의 안전성 확보조치 기준]을 모두 준수해야 한다

발송일
2012. 04

DB암호화를 하지 않기 위해 지켜야 하는

위험도분석표 26개 항목

원문보기

A안

DB접근통제가 Main인
위험도분석표 26개 항목을
모두 지킬 것이냐?

26개 조항중 하나라도 미이행시 DB암호화대상

B안

아니면 2012년 12월 말까지
고유식별정보 DB암호화를
완료할 것인가?

개인정보보호법고시 [개인정보의 안전성 확보조치 기준] 제7조 5항

내부망에 고유식별정보 저장시 암호화적용여부, 범위는 다음 기준에 따른다
1. (공공기관 경우) 영향평가 결과
2. (기업체 경우) 위험도분석 결과

[위험도분석]이란?
고유식별정보 DB암호화를 하지 않을 경우 개인정보처리자가
이행하여야 하는 최소한의 보호조치 기준으로
26개 항목 중 하나라도 [X]라면 DB암호화대상입니다.

(위험도분석표 26개 항목 중) 정책기반 5개 항목

No	정책기반	취지 / 해설
1	개인정보보호책임자지정	역할, 책임을 내부관리계획에 명시, 최고경영층으로부터 승인
2	개인정보보호정책 or 관리계획 (침해사고 대응계획 포함) 수립/운영	취지 체계적, 전사적 개인정보보호 수행 해설 침해 대응 계획 포함
3	외주인력 대상 보안서약서 집행, 비밀번호 노출예방	해설 [개인정보취급자]는 임직원, 계약직원, 아르바이트, 외부기관직원, 외부파견근로자 포함
4	DB서버 접속PC에서 정품 SW만 사용	취지 불법 S/W는 악성코드 침투 경로로 이용되므로 정품 사용
5	DB서버접근가능자 대상 연2회 교육실시	해설 집체교육, 인터넷교육, 그룹웨어교육, 위탁교육 모두 가능 (반드시 독립된 교육과정 or 교과목으로 수행)

(위험도분석표 26개 항목 중) 네트워크기반 6개 항목

No	네트워크 기반	취지 / 해설	기술적 보호조치
6	비인가 IP주소 접근통제	취지 〈개인정보처리시스템〉에 비인가접근을 차단, 개인정보불법사용/누출/변조/훼손 차단	
7	불필요한 서비스포트 사용통제	취지 불법침입의 경로로 이용될 수 있으므로 통제	
8	불법적인 해킹시도방지/ 모니터링	취지 침입차단/침입탐지기능을 갖춘 설비를 설치하고 상시 모니터링해야 함	
9	바이러스, 웜 등의 네트워크 유입차단	취지 해킹에 의한 개인정보 유출의 통로가 되므로 네트워크상에서 상시적으로 악성 프로그램 검사를 수행하여 유입을 차단	악성코드 배포사이트 접속차단 WebKeeper
10	네트워크 접속로그기록/ 주기적분석	취지 불법적인 접근행위 확인이 가능하고 유출사고 발생시 책임추적성 확보 해설 Access Log 등을 기록/백업하고 주기적으로 분석하여 이상징후를 파악하고 대응	네트워크 DLP Mail-i 인터넷접속 내역리포팅 WebKeeper
11	네트워크장비/ 정보보호시스템 보안패치	해설 환경설정,보안정책설정,침입패턴 등을 최신으로 유지	

(위험도분석표 26개 항목 중) DB/애플리케이션기반 13개항목

No	DB / 애플리케이션 기반	취지 / 해설	기술적 보호조치
12	네트워크를 통한 비인가자의 DB접근통제	해설 네트워크단 방화벽운용과 별도로 DB에 대한 비인가자의 접근통제 실시 상시적인 DB접속자 개개인식별을 위해 DB접근제어솔루션 사용권장	DB접근제어 (=DB방화벽, DB접근통제) 솔루션 DB-i
13	DB서버내 불필요 서비스포트 차단	취지 불법 침입경로 차단	
14	DB접속자/ 개인정보취급자 접속기록 저장	취지 책임추적성 확보 해설 DB관리툴, Telnet, Web or 응용프로그램 통한 접속기록 모두 저장	
15	DB접속기록 주기적 모니터링	취지 이상징후파악/조치, 모니터링을 알림으로써 불법적시도 최소화 해설 최소 주 1회 이상 모니터링 수행	

(뒷장에서 계속)

(위험도분석표 26개 항목중) DB/애플리케이션기반 13개항목 (앞장에서 계속)

No	DB / Application기반	취지 / 해설	기술적 보호조치
16	DB서버에 접속하는 관리자PC는 인터넷망과 망분리	취지 DB관리자PC가 악성코드에 감염, 해킹경로로 이용되는것을 막음 해설 물리적, 논리적 망분리 모두 가능	관리자PC 인터넷접속 차단으로 망분리효과제공 WebKeeper
17	DB 접근권한 차등화부여	취지 업무목적 외 접근차단 해설 업무수행목적에 따라 최소한의 범위로 차등화하여 부여	DB접근제어 (=DB방화벽, DB접근통제) DB-i
18	인사이동 발생시 지체없이 DB접근권한변경	취지 업무목적 외 접근차단 해설 공식적 사용자계정 관리절차에 따라 통제	
19	DB 로그인 비밀번호 최소 3개월마다 변경	해설 DB접속자, 개인정보취급자의 비밀번호를 3개월마다 강제변경	
20	DB로그인 비밀번호 5회이상 입력오류시 접근제한	취지 비밀번호무차별대입공격을 사용한 비밀번호 해킹 방지	
21	DB 및 DB접속어플리케이션 서버에 대한 물리적 접근통제	해설 전산실이 있을 경우 출입통제/내역 기록, 없을 경우 통제선, 칸막이 등을 이용	물리적보안
22	DB/DB접속 어플리케이션서버에서 보조기억매체사용시 관리자 승인	해설 보조기억매체의 악성코드 감염여부 확인 후 관리자승인 승인내역기록	Privacy-i (윈도우서버경우)
23	DB/DB접속어플리케이션서버에 접속하는 단말기 OS보안패치	취지 취약점을 악용하는 악성코드감염방지 해설 OS제조사 업데이트공지시 지체없이적용	DB-i
24	DB저장매체 불용처리시 (폐기,양여,교체 등) 개인정보 모두 파기	취지 개인정보유출을 막기 위해 복구될 수 없도록 삭제	

(위험도분석표 26개 항목중) 웹기반 2개 항목

No	웹(Web)기반 (웹사이트를 운영하는 경우에만 해당)	취지 / 해설
25	연1회이상 웹취약점 진단/보완 or 비인가자의 웹서버접근, 홈페이지위변조 상시적 자동차단	취지 해킹은 (대표적으로) 외부에 오픈되어있는 웹서버를 통해 발생하므로 보안필요
26	웹서버 프로그램&OS 대상 보안패치	취지 웹취약점을 이용하는 악성코드 감염방지

02

공공 · 공사 · 공단

발송일
2014. 04

행정자치부에서

공공기관 [개인정보보호관리수준진단]실시 2014년 진단평가항목 분석

2013년과 달라진 점 1 289개 ▶ 728개 공공기관으로 진단대상 대폭 확대

중앙부처 / 산하기관 348개

중앙부처 44개 — 〈시범기관〉 중앙부처산하기관50개

(〈시범기관〉을 제외한) 중앙부처산하기관 254개 → [정부업무평가]에 반영

자치단체 244개 (2013년 50개에서 대폭 증가)

광역자치단체 17개 / 기초자치단체 227개 → [지자체합동평가]에 반영

지방공기업 136개

지방공기업 136개 — 2013년 진단결과 특히 〈개인정보처리시스템〉 접근권한관리가 취약 → [지방공기업평가]에 반영

2013년과 달라진 점 2 침해사고대책 개선을 위해 4대 항목 중점개선

2013년 289개 기관 대상 평균점수 : 86.54 (지속개선 필요수준)

〈평가지표〉

- 관리체계 구축
- 보호대책 시행

(양호)

- 침해사고 대책 미흡 → 중점개선을 위해 가중치 상향

2014년 4대 중점개선항목

1. 9. 개인정보 노출방지 개선 (노출방지 모니터링 / 정기점검)
2. 10.개인정보 침해사고 대응절차
3. 11.1. 〈개인정보처리시스템〉 접근권한관리
4. 11.2 〈개인정보처리시스템〉 접속기록 정기점검 / 후속조치

2013년 진단결과 2014년에 가중치가 플러스된 침해사고대책 항목

9.1 홈페이지 개인정보 노출방지 모니터링 정기점검실시

진단항목	9.1 기관 홈페이지 개인정보 노출방지 모니터링, 정기점검을 실시하고 후속조치를 이행하는가?
세부설명	· 홈페이지 개인정보 노출방지 시스템 구축운영 · 상시모니터링체계 구축 · 홈페이지 개인정보노출/취약점 점검 정기적 실시 후 후속조치
행자부 제출 증빙자료	· 개인정보 노출방지 모니터링, 정기점검 후 업데이트 등 수행결과
행자부의 점수산정방법	①(20점) 개인정보보호 온라인 자가진단/후속조치 시행시 ②(10점) 노출방지 정기점검, 노출후속조치 이행 ③(5점) 노출모니터링 운영 ④(0점) 노출방지 체계 없음

기술적 보호조치

홈페이지 내 개인정보 온라인으로 정기적 노출점검, 상세리포트 제공

9.2 개인정보보호 자가진단 / 개선조치 수행

진단항목	9.2 [개인정보보호자가진단] 참여 및 그 결과에 따른 개선조치를 수행하였는가?
세부설명	개인정보보호 자가진단시스템(www.privacy.go.kr)을 통해 개인정보보호 관련 법규, 지침 등에 대한 준수상태 자율적 측정/미비점 개선조치 수행
행자부 제출 증빙자료	개인정보 자가진단 수행 확인서 및 그 결과에 따른 후속조치 내역
행자부의 점수산정방법	①(20점) 개인정보보호 온라인 자가진단 수행/후속조치 ②(10점) 개인정보보호 온라인 자가진단 수행 ③(0점) 자가진단 수행 않음

10.1 개인정보 침해사고 대응절차수립

진단항목	10.1 개인정보 유·노출 및 침해사고발생에 대한 대응절차를 수립하였는가?
세부설명	개인정보 유·노출 및 침해사고를 통한 사회적, 경제적 피해 등 2차 피해 예방을 위해 침해사고 대응 범위, 절차, 담당자, 부서별 업무, 피해구제 방법, 비상연락망, 연락체계 등의 절차 마련
행자부 제출 증빙자료	개인정보 침해사고 대응절차/지침서
행자부의 점수산정방법	①(20점) 4개 필수항목이 모두 반영된 대응절차 수립/운영 ②(15점) 3개 필수항목이 반영된 대응절차 수립/운영 ③(10점) 2개 필수항목이 반영된 대응절차 수립/운영 ④(5점) 1개 필수항목이 반영된 대응절차 수립/운영 ⑤(0점) 침해사고 대응절차 없음

10.2 개인정보 침해사고 대응절차전파

진단항목	10.2 대응절차를 개인정보취급자에게 전파하여 신속히 대응할 수 있는 체계를 구축하였는가?
세부설명	침해사고에 대비하여 개인정보취급자 대상 교육/모의훈련 실시, 사내 정보시스템(인트라넷) 게시 등으로 신속하고 효율적으로 대응할 수 있는 체계구축
행자부 제출 증빙자료	대응절차 전파 실적(문서/인트라넷 게시/교육/모의훈련 등)
행자부의 점수산정방법	①(20점) 침해사고 대응절차 전파(문서, 게시 등), 교육, 모의훈련 등 실시 ②(10점) 교육, 모의훈련을 통한 취급자 전파 ③(5점) 문서시행 or 인트라넷 게시 ④(0점) 침해사고 대응절차 전파 없음

11.1 〈개인정보처리시스템〉 접근권한관리

진단항목	11.1 〈개인정보처리시스템〉 접근권한을 관리하는가?	기술적 보호조치
세부설명	· 〈개인정보처리시스템〉 접근권한은 최소범위로 차등부여 · 접근통제조치 · 〈개인정보처리시스템〉 접근허용 및 취소를 위한 공식적 사용자등록 및 해지절차 마련 · 개인정보처리자는 인사이동시 지체없이 〈개인정보처리시스템〉 접근권한을 변경 or 말소	〈개인정보처리시스템〉별 접근권한관리 DB일 경우 DB-i
행자부 제출 증빙자료	[접근권한 관리 문서지침] · 기관별&시스템별 접근권한관리정책 포함 문서	WAS를 통한 DB접근 경우 was-i
행자부의 점수산정방법	①(20점) **〈개인정보처리시스템〉별 접근권한관리시** ②(5점) 기관별 접근권한관리정책운영 ③(15점) 시스템별 접근권한, 권한부여대상, 부여 해지절차 등을 문서로 관리 ④(-5점) 시스템별 접근권한 관리정책부실, 누락시 시스템당 -5점 감점	SAP을 통한 DB접근 경우 App-i

11.2 〈개인정보처리시스템〉 접속기록 점검/감사

진단항목	11.2 〈개인정보처리시스템〉 접속기록 점검/감사를 실시하는가?	기술적 보호조치
세부설명	접속기록은 불법접근, 불법행동을 확인할 수 있는 중요자료임 접속기록 백업은 개인정보DB무결성을 유지하기 위한 중요요소임 · 접속기록이 위변조, 도난, 분실되지 않도록 최소 6개월 보관 · 〈개인정보처리시스템〉 접속기록을 정기점검/감사하여 시스템 관리자 / 개인정보취급자들이 개인정보를 오남용하지 않도록 조치	〈개인정보처리시스템〉별 접속기록 점검 / 감사 ※ 이용자식별정보 (접속일시, ID, IP주소 등), 서비스이용정보 (생성,열람,수정,삭제,검색, 출력) 모두 감사
행자부 제출 증빙자료	〈개인정보처리시스템〉 접속기록점검, 분석내역, 후속조치내역	DB일 경우 DB-i
행자부의 점수산정방법	① (20점) 매년 50%이상 시스템점검, 점검결과에 대한 후속조치이행관리 ② (10점) 매년 50%이상 시스템 점검, 점검결과 조치이행실적 없음 ③ (15점) 일부시스템 점검 실시, 점검결과 후속조치 이행 확인 ④ (-5점) 일부시스템 점검 실시, 점검결과 후속조치 이행실적 없음 ※접속기록점검은 ① 이용자식별정보(접속일시, ID, IP주소 등), ② 서비스이용정보(생성, 열람, 수정, 삭제, 검색, 출력)를 모두 점검해야 인정	WAS를 통한 DB접근 경우 was-i SAP을 통한 DB접근 경우 App-i

2014년 관리수준 진단 평가항목

진단지표 및 가중치(3개 분야, 11개 지표, 23개 항목)

분야	진단지표	가중치				세부항목	기술적 보호조치
총계		100					
관리 체계 구축 (35)	1. 개인정보보호 기반마련	5		(8)		1.1 개인정보보호 전담조직과 적정 인력이 운영되고 있는가?	
						1.2 2014년도 개인정보보호활동수행에 필요한 예산을 반영하였는가?	
	2. 위탁업무에 따른 개인정보 보호활동	12		-		2.1 수탁업체대상 개인정보처리현황에 대해 관리·감독하고 있는가?	
						2.2 위탁계약에 따라 개인정보를 처리하는 경우, 법 의무사항에 대해 문서화하고 있는가?	
관리 체계 구축 (35)	3. 개인정보보호 교육추진	7		(12)		3.1 연간 개인정보보호 교육계획이 수립되어 있는가?	
						3.2 개인정보취급자, 일반 직원 등에 대한 교육이 모두 이행되고 있는가?	
	4. 개인정보보호 책임자의 역할수행	11		(15)		4.1 개인정보 보호책임자가 지정되고, 그 역할이 정의되어 있는가?	
						4.2 개인정보 보호책임자가 교육/관리/감독 등 역할을 수행하고 있는가?	
보호 대책 수립/ 시행 (30)	5. 개인정보 목적 외 이용·제3자 제공절차	8	(11)	(11)	(15)	5.1 개인정보목적 외 이용에 따른 절차, 개인정보 제3자 제공에 따른 절차를 수립하고 이행하는가?	
	6. 개인정보 파일관리	7	(9)	(10)	(15)	6.1 개인정보처리방침의 이력관리/ 현행화가 이루어지고 있는가?	PC내 개인정보점검 Privacy-i 서버내 개인정보점검 Server-i
						6.2 개인정보파일의 등록 및 변경이 철저하게 이루어지고 있는가?	
						6.3 개인정보파일 등록항목을 법에서 정한대로 하고 있는가?	
	7. 개인정보 영향평가 수행	7	-	(9)	-	7.1 개인정보 영향평가 수행 계획이 수립되어 있는가?	Privacy consulting
						7.2 개인정보 영향평가를 수행하고 있는가?	
	8.영상정보 처리기기 설치/운영	8	(10)	-	-	8.1 영상정보에 대한 이용, 제공, 열람 관리대장을 운영하는가?	
						8.2 영상정보처리기기 운영/관리방침에 법 의무사항이 모두 반영되어 있는가?	

(뒷장에서 계속)

2014년 관리수준 진단 평가항목 (앞장에서 계속)

진단지표 및 가중치(3개 분야, 11개 지표, 23개 항목)

분야	진단지표	가중치		세부항목	기술적 보호조치
총계		100			
침해사고 대책 (35)	9. 개인정보 노출방지 / 자율개선	10	(16)	9.1 개인정보 노출방지를 위한 모니터링, 정기점검을 실시하고 노출이나 취약점 발견시 후속조치를 이행하고 있는가?	홈페이지 노출개인정보 점검 / 파기
				9.2 '개인정보 자가진단' 참여 / 그 결과에 따른 개선조치를 수행하였는가?	
	10. 개인정보 침해사고 대응절차수립	12	(19)	10.1 개인정보 유·노출 / 침해사고 발생에 대한 대응절차를 수립하였는가?	
				10.2 대응절차를 개인정보취급자에게 전파하여 신속하게 대응할 수 있는 체계를 구축하였는가?	
	11. 〈개인정보처리시스템〉의 안전한 이용 / 관리	13	-	11.1 〈개인정보처리시스템〉의 접근권한을 관리하는가?	▶DB접근통제 DB-i
				11.2 〈개인정보처리시스템〉에 대한 접속기록 정기점검 / 후속조치가 적절히 이루어지는가?	▶웹어플리케이션을 통한 DB접근통제 was-i ▶SAP을 통한 DB접근통제 App-i

2014 금융권 유출사고 이후

행자부, 공공기관에 <개인정보처리시스템>별로 점검지시

NEWS

철저한 원인규명과 함께 근본적 대책을 마련하라
[아시아경제 2014.1.27]

2월 국회에서
개인정보보호 관련 국정조사, 청문회 개최

- 개인정보 관련 법 개정
- 행자부 대대적 실태점검/감사 예정

2014년 2월7일까지 행자부에 제출

공공기관 개인정보취급자
〈개인정보처리시스템별 자체점검항목/결과표〉 제출

공공기관 개인정보책임자
〈개인정보처리시스템별 자체점검항목/결과표〉를 〈개인정보 관리실태 자체점검표〉로 수합

행자부
검토/실사

〈개인정보처리시스템〉별로 개인정보 개수, 항목 모두 파악후 보고해야 함

〈개인정보처리시스템〉별 자체점검항목/결과표

자체점검항목은 법에 근거한 의무사항이기 때문에 위반으로 인한 개인정보유출시 형사처벌 대상임
개 인정보보호법

개선이 필요하다면?

분야	개 근거조항	세부점검항목	양호	개선 필요	해당 없음	기술적 보호조치
수집 · 이용 동의	15조	1. 온 · 오프라인 회입가입시 동의 여부		✓		Privacy consulting
		2. 각종 게시판, 기타 개인정보 수집시 동의 여부		✓		
		3. 정보주체 동의시 필수고지항목 고지 여부		✓		
		4. 필수고지항목의 적정성 여부 * 필수고지항목 4개: ①목적 ②항목③보유이용기간 ④거부권/불이익		✓		
최소수집 / 서비스제공 거부	16조	5. 목적에 필요한 최소한의 개인정보 수집 여부		✓		
		6. 최소한 정보외의 개인정보수집에 대한 미동의를 이유로 재화 or 서비스 제공거부 여부		✓		

(뒷장에서 계속)

〈개인정보처리시스템〉별 자체점검항목/결과표 (앞장에서 계속)

분야	개 근거조항	세부점검항목	양호	개선필요	해당없음	기술적 보호조치
제공	17조	7. 제3자에게 개인정보 제공시 정보주체 동의 여부		✓		Privacy consulting
		8. 정보주체 동의시 필수고지항목 고지 여부		✓		
		9. 필수고지항목의 적정성 여부 *필수고지항목 5개 : ①제공받는 자 ②목적 ③항목 ④보유이용기간 ⑤거부권/불이익		✓		
이용 · 제공 제한	18조	10. 수집당시 정보주체의 이용/제공 동의 범위를 초과한 이용/제공 여부		✓		
		11. 제공시 제공 목적범위내 이용, 안전조치실시, 목적달성 후 파기 등 요청여부		✓		
		12. 동의에 의한 목적 외 이용, 목적 외 제3자 제공시 필수 고지항목 고지여부		✓		
		13. 필수고지항목의 적정성 여부 *필수고지항목 5개 : ①제공받는 자 ②목적 ③항목 ④보유이용기간 ⑤거부권/불이익		✓		
파기	21조	14. 보유기간 경과, 처리목적달성 후 지체없이 파기		✓		Privacy-i · 유효기간설정 · 보유기간경과정보검색 · 복구재생불가한 파기
		15. 파기시 복구 or 재생되지 않도록 조치		✓		
		16. 임시파일/출력자료 등을 즉시 파기		✓		
		17. 법령에 따라 보존시 별도로 분리보관		✓		
동의받는 방법	22조	18. 최소개인정보와 그 외의 개인정보 구분 동의		✓		Privacy consulting
		19. 필수정보와 선택정보의 구분 동의		✓		
		20. 홍보를 위한 정보와 그렇지 않은 정보의 구분 동의		✓		
		21. 선택항목/홍보권유정보의 미동의를 이유로 재화/서비스 제공거부		✓		
민감정보 처리제한	23조	22. 사상, 정치, 건강 등 민감정보 수집/제공시 구분동의		✓		
		23. 정보주체 동의시 필수고지항목 (수집시 4개, 제공시 5개) 고지		✓		
		24. 필수고지항목(수집시 4개, 제공시 5개) 의 적정성여부				
고유식별정보 처리제한	24조	25. 고유식별정보의 동의에 의한 수집/ 제공시 구분동의		✓		
		26. 주민번호 외 회원가입방법 제공		✓		
업무위탁에 따른 처리제한	26조	27. 위탁계약시 문서(계약서)에 의한 계약여부		✓		Privacy consulting
		28. 문서(계약서)에 필수반영사항 포함여부 *필수반영사항 6개 : ①목적외 처리금지 ②기술/관리적 보호조치 ③목적/범위 ④재위탁 제한 ⑤접근제한 등 안전조치 ⑥관리/감독사항		✓		
		29. 수탁자에 대한 교육 실시여부		✓		
		30. 처리현황 점검 등 수탁자 관리감독여부		✓		

(뒷장에서 계속)

〈개인정보처리시스템〉별 자체점검항목/결과표 (앞장에서 계속)

분야	개 근거조항	세부점검항목	양호	개선 필요	해당 없음	기술적 보호조치
개인정보 취급자 감독	28조	31. 개인정보취급자에 대한 관리감독 (접근권한 관리/통제 등 포함)		✓		DB-i DB접근권한관리, 통제 was-i 웹애플리케이션을 통한 접근권한관리, 통제
		32. 개인정보취급자에 대한 보안서약서 징구		✓		Privacy consulting
		33. 개인정보취급자에 대한 정기적인 교육실시		✓		
내부관리계획 수립 · 시행		34. 내부관리계획 수립/시행 여부		✓		Privacy consulting
		35. 내부관리계획의 필수반영사항 포함 여부 * 필수반영사항 4개 : ①보호책임자지정 ②보호책임자 및 취급자의 역할/책임 ③안전성확보조치 ④취급자교육		✓		
접근권한관리/ 접근통제	29조 (안전 조치 의무)	36. 시스템접근권한을 필요최소한의 범위로 업무담당자에게 차등부여		✓		was-i 웹애플리케이션을 통한 개인정보오남용방지, 접근기록저장 · 외부 WAS를 통한 접속자 DB조회권한 제한 · 소량조회 반복하여 대량조회시 적발 · 정기적 접속기록 검색을 통해 과다조회자 추적 DB-i DB접근통제 · DB조회권한 관리 · 과다조회 부서/직원 점검
		37. 인사이동으로 취급자변경시 접근권한 변경 or 말소		✓		
		38. 접근권한 부여/변경/말소내역기록 관리 및 최소 3년보관		✓		
		39. 취급자별로 개별계정 발급		✓		
		40. 안전한 비밀번호 작성규칙의 수립 · 적용		✓		
		41. 불법적 접근/침해사고방지를 위한 시스템 설치 · 운영		✓		
		42. 외부에서 정보통신망을 통한 접속시 가상사설망, 전용선 등 안전한 접속수단 제공		✓		
		43. P2P/웹하드 등 비인가프로그램 공유설정 등에 대한 접속차단 실시		✓		WebKeeper P2P, 웹하드 접속차단
		44. 인터넷홈페이지의 개인정보노출방지를 위한 보안조치		✓		웹프라이버시 웹상 개인정보 필터링 서비스

(뒷장에서 계속)

〈개인정보처리시스템〉별 자체점검항목/결과표 (앞장에서 계속)

분야	개 근거조항	세부점검항목	양호	개선필요	해당없음	기술적 보호조치
개인정보의 암호화	29조 (안전조치 의무)	45. 개인정보 암호화계획 수립/시행		✓		· DB암호화 솔루션 DB-i, was-i 전송시 암호화 Server-i, Privacy-i 저장시 암호화
		46. 비밀번호의 외부 송수신 시 암호화		✓		
		47. 비밀번호의 내부저장 시 일방향 암호화		✓		
		48. 바이오정보의 외부 송수신 시 암호화		✓		
		49. 바이오정보의 내부 저장 시 암호화		✓		
		50. 고유식별정보의 외부 송수신 시 암호화		✓		
		51. 고유식별정보의 인터넷과 내부망의 중간지점(DMZ) 저장시 암호화		✓		
		52. 고유식별정보 내부저장시 암호화 or 상응하는 조치		✓		
접속기록의 보관		53. 취급자의 접속기록을 최소 6개월 이상 보관		✓		was-i 웹애플리케이션을 통한 접근기록저장 DB-i · DB접속기록 저장 · 과다조회 부서/직원 점검 · ID, 날짜, 시간, IP, 업무 (열람, 수정, 삭제, 인쇄, 입력 등) 모두 기록
		54. 접속기록항목이 적정한지 여부 * 접속기록항목 4개 : ① ID ②날짜/시간 ③ 접속자 IP 주소 ④ 수행업무(열람, 수정, 삭제, 인쇄, 입력 등)		✓		
		55. 접속기록이 위/변조 , 도난, 분실되지 않도록 안전보관		✓		소만사 전 솔루션은 위변조방지스토리지 탑재
보안프로그램 설치/운영		56. 보안 프로그램의 설치/운영 여부		✓		
		57. 보안프로그램 자동업데이트 or 일 1회 이상 업데이트		✓		
물리적 접근 방지		58. 전산실, 자료보관실 등 물리적보관장소 출입통제절차 수립/운영		✓		Privacy-i 개인정보출력물 이력관리
		59. 개인정보서류, 보조저장매체 등을 잠금장치 있는 안전한 장소에 보관		✓		
개인정보 처리방침 수립/공개	30조	60. 개인정보 처리방침의 수립 여부		✓		Privacy consulting
		61. 개인정보처리방침에 필수항목 포함 여부 * 필수항목 8개 : ① 처리 목적 ② 처리/보유기간 ③ 제3자 제공사항(해당시) ④ 위탁사항(해당시) ⑤ 정보주체 권리의무 / 행사방법 ⑥ 처리항목 ⑦ 파기사항 ⑧ 안전성확보조치		✓		
		62. 개인정보처리방침의 홈페이지 등 공개 여부		✓		
개인정보 보호책임자 지정	31조	63. 개인정보보호책임자 지정 여부		✓		
		64. 개인정보보호책임자의 업무 범위, 자격요건 등 적정성 여부		✓		

발송일
2013. 11

한쪽에선 보안하라 하고
한쪽에선 개방하라 하는 때,

공공기관 개인정보취급자에게는
빅데이터에서 개인정보를 빨리, 정확하게
검출하는 능력이 꼭! 필요합니다

2013년 10월 31일,
행자부 [공공데이터의 제공 및 이용 활성화에 관한 법률] 시행에 따라

[공공정보 개방/공유에 따른 개인정보보호지침] 시행

원문보기

공공기관 개인정보 취급자는 무엇을 해야 하는가?

행복한 대한민국을 여는 정부 3.0
[개방 · 공유 · 소통 · 협력]

개인정보는
공공정보개방대상에서 **배제**

앞으로 공공기관내 정보는
개방/공유가 원칙

(이미 공개된 다른 정보와 결합해서)
개인 식별성이 있는
'**개인정보화**'되지 않도록 해야 함

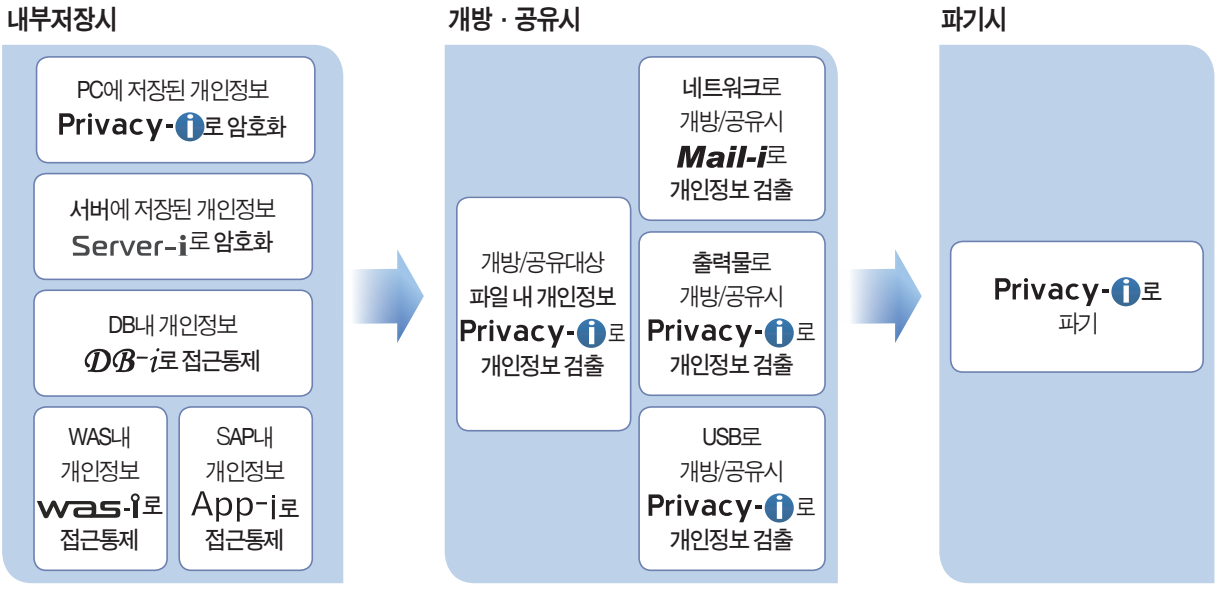
공공기관 개인정보 취급자는

공공정보 개방/공유 전에 반드시
개인정보 및 개인정보가 될 수 있는 정보를
검출 → 분석 → 파기/비식별화해야 함

개인정보 비식별화 방법

기법	비식별화 방법
가명처리	개인정보 중 주요식별요소를 **다른 값으로 대체**, 개인식별 차단 ex) 홍길동, 35세, 서울거주, 한국대 재학 → 임꺽정, 30대, 서울거주, 국제대 재학
총계처리 or 평균값대체	**데이터 총합 값**을 보임으로서 개별 데이터값을 보이지 않도록 함 ex) 임꺽정 180cm, 홍길동 170cm, 이콩쥐 160cm, 김팥쥐 150cm → 물리학과 학생 키 합: 660cm, 평균키 165cm
데이터값 삭제	데이터공유 및 개방 목적에 따라 데이터 셋에 구성된 값 중에 **필요없는 값 or 개인식별에 중요한 값을 삭제** ex) 홍길동, 35세, 서울, 한국대졸업 → 35세, 서울 ex) 주민번호 901206-123456 → 90년대생, 남자 ex) 개인관련 날짜정보는 연 단위 처리 ex) 유명인 가족정보, 판례 / 보도 등에 따라 공개된 사건과 관련됨을 알 수 있는 정보
범주화	데이터값을 **범주값으로 변환**하여 명확한 값을 감춤 ex) 홍길동, 35세 → 홍씨, 30대
데이터마스킹	공개된 정보 등과 결합하여 개인을 식별하는데 기여할 확률이 높은 주요 **개인식별자료를 보이지 않도록 처리**하여 개인을 식별하지 못하도록 함 ex) 홍길동, 35세, 서울, 한국대 재학 → 홍**, 35세, 서울, **대 재학

개인정보의 안전성 확보조치



국방부 산하기관 적용

[국방개인정보보호관리지침] 2012년 4월2일부터 시행

원문보기

[국방개인정보보호관리지침]이란?

[개인정보보호법]과 [표준개인정보보호지침]에 따라
국방부, 합참, 각군, 국직기관, 소속기관 / 외부위탁업체가 지켜야 할 개인정보보호지침

제 5장 개인정보의 기술적 보호조치

조항	내용	기술적 보호조치
28조 물리적접근제한	① 개인정보와 〈개인정보처리시스템〉의 잠금장치 등 물리적 접근방지조치 ② 출입사실/열람내용에 관한 관리대장 작성 ③ 관리대장의 출입/열람내용 주기적검토	물리적 접근방지
29조 출력 복사시 보호조치	① 개인정보 출력/복사시 유출방지조치 ② 민감 or 다량의 개인정보 출력/복사시 성명, 일시 등을 기재, 책임소재확인 ③ 분쇄/소각 등 안전한 방법으로 파기	Privacy-i · 개인정보출력시 결재 or 차단 · 출력자명, 일시, 파기날짜 인쇄 · 파기리포트 제공
30조 개인정보취급자 접근권한관리/ 인증	① 〈개인정보처리시스템〉 접근권한을 최소인원에게 부여 ②개인정보 접근권한(읽기/쓰기/수정/삭제) 차등부여 ③인사변경시 지체없이 〈개인정보처리시스템〉 접근권한변경 ④통신망으로 외부에서 〈개인정보처리시스템〉접속시 공인인증서 등 안전한 인증수단 적용 ⑤권한부여, 변경, 말소내역 기록, 5년간 보관	DB-i · DB접근권한관리 · 외부접속시 암호화채널 제공 · 위변조방지 스토리지 제공
31조 암호화	① 고유식별번호는 안전한 암호알고리즘으로 암호화저장 ②비밀번호 / 바이오정보는 일방향 암호화저장 ③정보통신망(인터넷,국방망,전장망등)으로 개인정보 송수신시 보안서버구축등으로 암호화 ④개인정보 PC저장시 암호화	Privacy-i · 국정원인증 암호화알고리즘으로 암호화
32조 접근통제	① 불법접근/침해사고 방지를 위해 다음 기능포함 시스템 운영 1. 접속권한을 IP 주소 등으로 제한 2. 접속IP주소 등을 재분석, 개인정보유출시도 탐지 ② 「군사보안업무훈령」 제120조를 따라 비밀번호 관련 보안규칙준수 ③ 홈페이지, 공유설정등으로 개인정보가 공개되지 않도록 개인정보처리시스템/PC에 조치	DB-i DB접근통제기능
33조 접속기록의 위/변조 방지	① 〈개인정보처리시스템〉에 접속, 개인정보처리시 접속기록을 저장 ② 접속기록에 대해 분기1회 이상 정기적으로 확인, 감독 ③ 위변조방지를 위해 접속기록을 별도의 저장매체에 최소 2년 백업보관	DB-i 접속기록저장/ 위변조방지 스토리지제공
34조 보안프로그램의 설치/운영	① 개인정보를 PC에서 취급할 경우 백신 등의 보안프로그램 설치/운영 ② 보안 프로그램은 최신버전으로 업데이트적용 ③ 자동업데이트설정/실시간 감시기능 적용	

기타 중요규정

조항	내용
3조 용어	2. "국방개인정보처리자" (이하 처리자) : 국방부(각 국실), 합참, 각 군/기관, 한시기구 3. "개인정보보호책임관" (이하 보호책임관) : 개인정보보호업무총괄지휘자로 국방부, 합참, 각군/기관별 총괄책임자 4. "개인정보보호담당자" (이하 보호담당자) : 개인정보보호책임관을 보좌하는 실무자 5. "개인정보처리책임자" (이하 처리책임자) : 개인정보취급부서의 장으로 해당개인정보처리의 총괄책임을 지는 자
4조 개인정보보호 원칙	① 최초수집부서가 개인정보보호관리책임을 진다.
5조 개인정보보호 책임관 지정	① 보호책임관/보호담당자 지정 및 매년 1월 국방부 정보화기획관실에 보고 (변경발생시 15일 이내 보고) ② 개인정보 보호책임관의 자격은 3급 or 대령급 이상
8조 개인정보처리 방침 수립/승인	③ 개인정보처리시스템 및 행안부에 등록 및 개인정보파일(PC파일,종이문서)대상 개인정보처리방침수립
9조 개인정보처리 방침 공표	① 보호책임관은 개인정보파일 자체평가 후 파일대장을 국방부 정보화기획관실에 관리등록요청, 행안부 등록대상 개인정보파일은 국방부 정보화기획관실을 통하여 행안부에 등록
14조 개인정보신규 수집, 변경시 자체평가	개인정보 수집, 변경시 다음 자체평가실시 1. 개인정보파일에 대한 처리책임자/ 취급자지정여부 2. 보유목적/관련근거의 적절성 3. 보유항목/보유기간의 적절성 4. 개인정보 이용, 제공부서 범위의 적절성 5. 개인정보에 대한 안전성 확보의 적절성
21조 파기	① 파기사유발생시 파기/파기관리대장 작성, 보호책임관에게 보고 ② 행안부등록대상 파일파기시 보호책임관은 행안부에 파기사실등록 및 국방부 정보화기획관실에 승인요청 ③ 복구 or 재생이 되지 않도록 파기
25조 개인정보 침해사고	① 개인정보 침해사고 인지시 국방부 정보화기획관실에 유출된 개인정보 항목, 유출시점과 경위, 피해최소화방법,대응조치 보고 ② 5일 이내, 정보주체에게 유출통지

03

정보통신서비스 제공자

발송일
2015. 01

2015년 5월 19일, 오늘부터 시행됩니다!

정보통신망법고시 [개인정보의 기술적 관리적 보호조치기준] 개정시행

본 뉴스레터는 5.15일 열린 [개인정보의 기술적 관리적 보호조치기준] 주요개정내용 설명회 기준으로 작성되었습니다

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

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 보호조치에 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

정보통신망법고시 [개인정보의 기술적 관리적 보호조치 기준]

〈관리적 보호조치 기준〉

조	내용	기존과 달라진 점	관리적 보호조치
1조 목적	① 법 제28조 1항 및 시행령 15조 6항에 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 정기적으로 교육실시 입법예고 후 추가 1. 교육목적/대상 2. 교육내용 3. 교육일정/방법	**변경** 매년 2회 이상 → 사업규모, 개인정보 보유수 등을 고려하여 정기적으로	

(뒷장에서 계속)

정보통신망법고시 [개인정보의 기술적 관리적 보호조치 기준]

〈기술적 보호조치 기준〉

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 ①,②항에 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 대통령령 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

(뒷장에서 계속)

정보통신망법고시 [개인정보의 기술적 관리적 보호조치 기준]

〈기술적 보호조치 기준〉 (뒷장에서 계속)

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, 정기백업 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 SSL(Secure Socket Layer)인증서 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

발송일
2014. 12

유출되지 않아도 개인정보 미파기자체를 형사처벌!

정보통신망법개정안 개인정보 미파기죄 신설

2014. 11월 29일부터 2015년 현재 시행 중입니다

개 인정보보호법 신 용정보법 정 보통신망법 전 자금융거래법

본 레터는 테크앤로 교육을 수강한 후 강의내용을 참고하여 작성하였습니다

2014년 금융권유출사고 근본원인 중 하나는 〈개인정보 미파기〉

유출정보 상당수가 **유효기간 지난 개인정보**

특히, 여러 사람이 접근하는 **DB, 서버 내 〈개인정보 미파기〉가 위험**

DB 내 개인정보를 외주업체직원이 **USB로 유출**

2014~2015년은 개인정보 〈점검→파기〉의 해

유효기간 지난 개인정보가 파기되지않고 쌓여있는 것이 **적폐**

어떤 개인정보가 어디에 얼마나 있는지 모르는 것이 **비정상**

개인정보 〈점검→파기〉를 주내용으로 범정부 〈종합대책〉 발표

범정부연합
금융회사 개인정보유출 재발방지 종합대책
개정예정 개 신 전

국무총리실 범정부 TF
개인정보보호 정상화종합대책
국가적 개인정보대청소 선포
개정예정 개 신 정

법령근거없는 주민번호 **〈점검→파기〉** 시작 개 정

2015년은 **적폐해소 비정상의 정상화**의 원년

〈점검→파기〉하지 않으면 범죄! 유출과 동일한 형사처벌

〈개인정보 미파기〉에 2년 이하 징역, 2천만원 이하 벌금 조항 신설 (제73조 1의2호)

개인정보미파기1
〈수집이용목적 달성 개인정보〉 〈유효기간 끝난 개인정보〉 미파기

개인정보미파기2
법이 정한 파기방법 미준수

정보통신망법 제73조 제1의2호 (벌칙)
(정보통신망법 29조 1항을 위반하여)
개인정보를 파기하지 아니한 자를
2년 이하 징역 or 2천만원 이하 벌금에 처한다

정보통신망법 제29조 제1항 (보유이용기간 끝난 개인정보의 파기)
개인정보 보유,이용기간이 끝났거나 수집이용목적이 달성되면
복구/재생할 수 없도록 파기해야 한다

개인정보 미파기죄의 적용대상은 어디인가?

2015년 현재 정 적용대상에게 적용
정보통신망을 영리로 사용하는
273만개 사업자와 160만개 스마트폰앱

개 〈개인정보 미파기〉시 과태료 3천만원 이하

신 국회에서 개정중

예측 [개인정보보호 정상화 종합대책]에 따라
개 신에 도입될 가능성 존재

장기적으로 개 신 정 간
법적정합성 일치 및 법적용대상 명확화 예정

정 적용대상자 축소예정
전기통신/통신판매사업자
(37만개 사업자 +160만개 스마트폰앱)

개인정보 미파기죄는 양벌규정이 적용되므로 CEO 리스크임

정보통신망법 제75조 (양벌규정)

② 법인의 대표자나 법인의 대리인, 사용인, 종업원이 그 법인 또는 개인의 업무에 관하여 71조, 72조, 74조1항, 73조의 위반행위를 하면 행위자를 벌하는 외에 법인에게도 벌금형을 과(科)한다

BUT

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

제73조 1의2호 〈개인정보 미파기〉 발생시

위반 행위의 〈행위자〉식별	직원 or 외주직원의 고의/과실이 원인일 때	2014년 이후 법의 판단은 CEO의 책임에 초점	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: 직원 or 외주직원 형사처벌 / 법인처벌: 법인은 벌금형		행위자처벌: CEO 형사처벌가능 / 법인처벌: 법인은 벌금형

기업은 어떻게 대처해야 하는가?

1. 파기절차/방법을 포함한 〈개인정보취급방침〉 공개 (정보통신망법 제27조의2에 따라 위반시 과태료 3천만원)
2. 개인정보 미파기 **4대위험ZONE** 점검

1 DB → 2 서버 (2014년에 위험도증가) → 3 PC → 4 PC에서 복제된 정보 (출력물, USB)

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

CPO에게 보고 → CEO에게 보고

발송일
2014. 12

개정 정보통신망법 5대 변화
(2014년 11월29일부터)

1. 개인정보 미파기죄 신설

(유출되지 않아도)
개인정보 미파기시
(유출과 동일한) **형사처벌**

2. 망법고시[개인정보의 기술적 관리적 보호조치기준]위반으로 유출시

고객피해 입증없이도 손해배상 인당 **최대 300만원** + **2년** 징역 **2천만원** 벌금 + **매출의 3%** 과징금

3. 유출사고발생시

24시간 이내 이용자에게 고지
방통위 or **한국인터넷진흥원에 신고**

4. CISO 의무지정 후
미래부에 신고

5. 민감정보
정의확대 및 최소수집

1. (유출되지 않아도) 개인정보 미파기시 (유출과 동일한) 형사처벌

형사처벌 / 과태료

2015년 현재 시행중

〈목적달성 or 유효기간 끝난 개인정보〉 미파기시
정보통신망법 제73조 1의2호

형사처벌 2년징역or 2천만원벌금 이하

2015.08.18부터 휴면기간 1년으로 단축

〈휴면기간 종료된 개인정보〉 미파기시
정보통신망법 제73조 1의2호

과태료 3,000 만원 이하

2. 망법고시 [개인정보의 기술적 관리적 보호조치기준] 위반으로 유출시

손해배상, 형사처벌 및 과징금

2015년 현재 시행중

고객의 피해입증이 **불가**한 경우

법정손해배상

1인당 **최대 300만원**

정보통신망법 제32조의 2

피해고객이 유리한 방식 선택

[정상화대책]에서 시행예고

고객의 피해입증이 **가능**한 경우

징벌적손해배상

1인당 **피해액의 3배까지**

국무총리실 범정부TF [개인정보보호 정상화대책]

1천만명 개인정보유출시 손해배상액 **30조원**

손해배상 청구절차는?

개인정보 유출사고 발생 → 고객 손해배상 청구 → 기업 피해정도와 증거를 조사 배상액 산정,지급 → **기업** 고의 · 과실이 없었음을 입증 입증 못하면 배상

망법고시 [기술적 · 관리적 보호조치]를 위반한 경우 고의 · 과실이 없음을 입증하기 어려움

2015년 현재 시행중

형사처벌

2년징역 or 1천만원벌금 (이전)

→ **2년 징역 or 2천만원 벌금** 이하 (현재)

정보통신망법 제73조 1호

2015년 현재 시행중

과징금

매출의 1%까지 (이전)

→ 위반행위관련 **매출의 3%**까지 (현재)

정보통신망법 제64조의3 1항 6호

형사처벌 집행절차는?

개인정보 유출사고 발생 → 검사 벌금액(형량)을 정하여 법원에 약식기소 → **법원** (피고인 법정소환없이) 수사기록만 검토하여 유 · 무죄여부 / 벌금액 결정 → 처벌 2년이하 징역 / 2천만원이하 벌금

과징금 부과절차는?

개인정보 유출사고 발생 → **법원** 기술적 · 관리적 보호조치 위반여부 검사 → 법원 위반시 피해입증 절차없이 과징금 산정 → 처벌 매출액 3% 이하 과징금

60p [개인정보의 기술적 관리적 보호조치 기준] 규정 보기

유출사고발생시 손해배상, 형사처벌, 과징금을 피하기 위해
정보통신망법고시 [개인정보의 기술적 관리적 보호조치 기준]을 모두 준수해야 한다

3. 유출사고 신고규정 강화

유출사고발생시 24시간 이내 이용자에게 고지 및 방통위 or 한국인터넷진흥원에 신고

개정전 정보통신망법 제27조의3

개인정보분실 · 도난 · 누출시
· 지체없이 해당 이용자에게 고지
· 〈방송통신위원회〉에 신고

개정후

2015년 현재 시행중

24시간이내 유출사고 고지,
〈방송통신위원회〉 or 〈한국인터넷진흥원〉에 신고

24시간 이내로 고지, 신고하지 못한 경우
방송통신위원회에 소명자료 제출

참고) 개인정보보호법은 현재 유출사고 발생시 지체없이(=5일 이내)
고지 · 신고할 것을 규정하고 있음

4. CISO 의무지정 후 미래부에 신고

CISO 지정요건

개정전 정보통신망법 제45조의3

정보통신서비스제공자는
임원급 정보보호 최고책임자(CISO)를
지정할 수 있다

개정후

종업원 · 이용자 수 등이
대통령령 기준에 해당하는 정보통신서비스 제공자는
CISO 지정 후 **미래부 장관**에게 신고

(CISO를 지정해야하는) **대통령령 기준에 해당하는 정보통신서비스 제공자**

정보통신망법 대통령령 제36조의6 (정보보호 최고책임자 지정 · 신고 대상자의 범위)

(방통위 심의를 받는) 내용선별SW(유해차단프로그램) 개발/보급 사업자	ISMS인증을 받아야 하는 사업자	직원수 5명, 이용자 1천명이상 특수유형 온라인서비스제공자 (파일공유, P2P 등)
직원수 5명이상 통신판매업자	(PC방 게임방 사업자 대상) 음란물, 사행성게임 차단프로그램 제공자	직원수 1천명 이상 사업자

5. 민감정보 정의확대 및 최소수집

민감정보 정의 확대

개정전 정보통신망법 제23조

사상, 신념, 과거병력 등
개인의 권리 · 이익이나 사생활을
뚜렷하게 침해할 우려가 있는 개인정보

개정후

+ 가족 / 친인척 관계,
학력, 기타 사회활동경력

민감정보는 필요범위 내에서 최소수집

개정전 정보통신망법 제23조

이용자 동의를 받거나 법령상 허용된 경우
민감정보 수집가능

개정후

정보주체의 수집동의를 받아도
필요범위 내에서
최소한으로 수집가능

유출사고 발생시 CEO의 역할이 왜 중요한가?

바로가기

출처 : 구태언 테크앤로 대표변호사 칼럼

사고발생 후 **24시간**은 회사 존망을 가르는 **골든타임**

CEO만이 모든 부서를 아우를 수 있음

CEO만이 할 수 있는 일

신속한 〈상황실〉 설치 및 〈상황실장〉 역할수행

모든 정보가
상황실을 통해
CEO에게 집적되어야 함

위기상황에서 명확한 〈권한위임체계〉 수립

〈사전매뉴얼〉에 따른
명확한 권한위임체계 수립

단일한 의사결정

개인정보유출사고는
최고등급사고로 많은 의사결정 발생
예) 법적이슈, 현장조사, 언론취재,
상장기업 공시업무 등

사고발생시 CEO가 **간과**할 수 있는 부분 : **통지/신고**

통지/신고를 소홀히 할 경우, 향후 손해배상소송에서 불이익 발생

정보통신망법 제 27조의3 (개인정보누출 통지 · 신고)

유출사고 발생시
24시간이내 이용자에게 유출사고 고지 및
방송통신위원회 또는 한국인터넷진흥원에 신고
24시간 이내로 고지 · 신고하지 못한 경우
방송통신위원회에 소명자료 제출

(정당한 사유없이 경과시) **과태료 3천만원**

개인정보보호법 제 34조 (개인정보 유출통지 등)

유출사고 발생시 **지체없이**
이용자에게 유출사고 고지 및 **안전행정부 또는**
한국정보화진흥원, 한국인터넷진흥원에 신고

(정당한 사유없이 경과시) **과태료 5천만원**

발송일
2014. 12

2014년 11월 3일부터 시행! 정보통신망법 미래창조과학부 고시

[정보보호 관리등급 부여에 관한 고시]

원문보기

누가 신청하는가? ISMS(정보보호관리체계)인증을 3년 연속 유지한 조직

누가 심사하는가? 미래창조과학부 & 한국인터넷진흥원

심사절차는 어떻게 되는가?

ISMS인증을 3년 이상 유지한 조직 → [우수 or 최우수등급기준]을 모두 준수하는 〈정보보호관리체계〉 1년 이상 운영 → 한국인터넷 진흥원에 신청 → 〈1차〉 서면심사: 정책·지침·절차, 이행증적자료, 정보보호대책 적용여부 확인 → 〈2차〉 현장심사: 서면심사결과, 담당자 면담, 관련시스템확인, 취약점점검

기준을 모두 만족할 경우 어떤 등급을 받게 되는가?

최우수등급		우수등급	

등급의 유효기간은 얼마나 되는가? 1년

등급획득시 혜택은 무엇인가?

- 개인정보 유출사고발생시 **행정처분 감경**
- **개인정보**를 **안전**하게 **관리**하는 기업으로서 **공식적 인정받음**
- 등급을 홍보에 활용 **고객신뢰도** 향상

정보보호관리등급 세부평가기준

해당기준을 **모두 준수**해야 함 **최우수등급기준**은 **우수등급기준**을 **포함**

정보보호 전담조직 & 예산

구분	우수등급기준	최우수등급기준 (우수등급기준포함)
전담조직	이해당사자(ex IT조직 , 운영조직) 로부터 독립된 정보보호전담조직 구성, 공식적 직제규정	
전담인력	최근 1년 IT 인력대비	
	최소 5%, 최소 3명이상	최소 7%
예산	최근 3년 IT 예산 대비 전년 & 당해 정보보안예산	
	최소 7%	최소 10%
현황공개	정보보호활동, CSO역할 및 책임, 인증현황을 매 사업연도 종료 후 1달내 홈페이지에 공시	

정보보호관리활동

분야	항목	우수등급기준	최우수등급기준 (우수등급기준포함)	기술적 보호조치
정책수립 범위설정	1.1 정책수립	CEO가 정보보호 의지를 표명해야 한다 ex) 정보보호선언문		Privacy consulting
책임/조직	2.1 경영진참여	CEO에게 주기적으로 정보보호에 대해 보고해야 한다		
		분기별 1회 이상 보고	월 1회 이상 보고	
위험관리	3.1 방법/계획	위험관리를 주기적으로 수행해야 한다		
		· 반기별 1회 이상 수행 · 환경변화시 ex) 신규서비스런칭	실시간 위험분석체계 수립	
	3.2 식별/평가	전담인력의 〈위험관리방법/이력〉 지속관리절차 수립 [포함내용] 관리적 · 기술적 · 법적 위험분석 방법론, 시나리오기반 위험분석, 위험식별시 회의후 조직적대응		
대책구현	4.1 효과적 구현	CSO에게 정보보호대책 시행결과 보고 분기별 1회 이상 [포함내용] 계획대비진척도, 수준향상정도, 잔존위험여부, 이행목표 관리방안 등		
사후관리	5.1 법적요구사항 준수검토	〈법령+보안동향 포함 보고서〉발간→정보보호/시스템부서, CSO 포함 경영진과 공유		
		분기별 1회 이상 공유	월 1회 이상 공유	
		법준수여부 검토시 전문인력(변호사, 법무팀) 포함		
	5.2 운영현황관리	CSO대상 〈운영현황 검토→문제점, 개선안 등 효과성 검토결과〉 보고		
		반기별 1회 이상 보고	분기별 1회 이상 보고	
	5.3 내부감사	정보보호조직과 독립적으로 〈내부감사→보안조치계획 수립 이행여부감사〉 수행		
		독립수행주체가 TFT	독립수행주체가 감사조직	

정보보호관리등급 세부평가기준

정보보호조치수준

<table>
<tr><th>분야</th><th>항목</th><th>우수등급기준</th><th>최우수등급기준 (우수등급기준포함)</th><th>기술적 보호조치</th></tr>
<tr><td rowspan="3">정책</td><td rowspan="2">1.1
승인/공표</td><td colspan="2">〈정책 및 시행문서〉 제/개정시
①관련부서장 동의(서명) → ②법적준거성검토
→①, ②번을 위한 공식절차수립 및 승인이력유지 ex) 전자결재</td><td rowspan="10">Privacy consulting</td></tr>
<tr><td colspan="2">CEO가 전직원 대상 제/개정 내용 공표</td></tr>
<tr><td>1.2
유지/관리</td><td colspan="2">〈정책 및 시행문서 검토계획〉 수립·이행시
① 모든 지침 연1회 이상 검토
② 위험평가/내부감사시 〈정책 및 시행문서〉 제/개정 검토</td></tr>
<tr><td rowspan="5">조직</td><td rowspan="4">2.1
조직체계</td><td colspan="2">〈CSO 임명조건〉
① (예산,인력 집행권한이 있는)이사 or 임원급
② 인사정책에 CSO 경력/자격 규정/공식적 임명</td></tr>
<tr><td>〈정보보호전담조직〉의 80%이상
정보보호자격증 보유</td><td>· 〈정보보호전담조직〉 실무부서장
경력/자격기준을 인사정책에 규정/시행
(정보보호경력 5년 이상 or 자격증보유)</td></tr>
<tr><td colspan="2">〈정보보호위원회〉 업무 명문화
[포함내용] 정보보호지표현황, 최신이슈검토, 내부진단/감사결과, 추진실적, 투자사항, 정책/지침변경</td></tr>
<tr><td colspan="2">(CSO를 포함한) 〈정보보호위원회〉 주기적 개최
↓ 분기 1회 이상 개최 ↓ 월 1회 이상 개최
(보안담당자로 구성된) 실무협의회 월 1회 이상 운영,
의사결정필요시 〈정보보호위원회〉로 상정</td></tr>
<tr><td>2.2 역할&책임</td><td colspan="2">정보보호담당자 성과평가에 정보보호항목 포함</td></tr>
<tr><td rowspan="2">외부자
보안</td><td>3.1
요구사항정의</td><td colspan="2">외부자계약시 〈외부자보안준수 요구사항을 위한 별도절차〉를 지침 등 정책으로 수립
[포함내용] 외부자보안요구사항 검토절차, 위반시 벌칙</td></tr>
<tr><td>3.2
이행</td><td colspan="2">외부자 보안이행 점검 → 결과기록, 보고
<table>
<tr><th>계약기간</th><th>외부자 자체점검</th><th>외부자보안 이행감사/보고</th></tr>
<tr><td>1년 이상</td><td>월 1회</td><td>연 1회</td></tr>
<tr><td>1년 이하</td><td>월 1회</td><td>계약만료 전 1회</td></tr>
<tr><td>1개월 이하</td><td colspan="2">계약만료 전 1회</td></tr>
</table></td></tr>
<tr><td rowspan="2">정보
자산
분류</td><td>4.1
식별/책임</td><td colspan="2">법률상 보호조치가 의무화되는 정보자산 별도식별
[관리대상] 정보자산목록 실시간현황, 구성정보, 위치, 보안등급 등
↓ 〈자동화된 자산관리시스템〉으로 관리 ex) RFID or 바코드
↓ 〈SW관리체계〉 수립 ex) 저작권관리체계, 변경관리체계
〈데이터자산관리체계〉 수립 ex) 데이터흐름중심관리체계
최신성유지와 보안등급 재검토를 위한 정보자산실사 반기별 1회</td><td>정보자산식별
[DB][서버]
Server-i
[PC]
Privacy-i
데이터흐름중심보안
DLP+Center</td></tr>
<tr><td>4.2
분류/취급</td><td>문서(전자문서포함) 유출방지조치
ex) 암호화, 워터마킹, 네트워크DLP</td><td>정보유출통제시스템 우회경로 식별
→ 대응방안 수립</td><td>[네트워크DLP]
Mail-i™
[엔드포인트DLP]
Privacy-i
데이터흐름중심보안
DLP+Center</td></tr>
</table>

(뒷장에서 계속)

정보보호관리등급 세부평가기준

정보보호조치수준 (앞장에서 계속)

분야	항목	우수등급기준	최우수등급기준 (우수등급기준포함)	기술적 보호조치
교육	5.1 교육 프로그램 수립	연간 교육계획(대상, 교과구분) 수립 → CSO 보고		Privacy consulting
		(개인정보포함) 정보보호직무자 대상 전문교육 정보보호직무자는 연 40시간, IT직무자는 연 8시간 이상		
		인식재고활동 수행 ex) 소책자, 캠페인, 포스터, 보안의 날 지정, 뉴스레터 등		
	5.2 교육시행 / 평가	전직원 교육 반기1회 이상	온라인시스템으로 상시교육체계 운영	
		교육시행결과를 CSO에게 보고	교육참여도를 성과평가반영	
인적보안	6.1 책임	주요직무자현황(변경추이포함) 파악 → CSO 보고 반기 1회 이상		
	6.2 인사규정	관련부서(인사/정보시스템/정보보호부서 등)와 퇴직 및 직무변경정보 공유		[DB] DB-i
		정보시스템 접근권한 자동화시스템	정보시스템 접근권한 회수체계	
		정보보호책임/의무를 모든 임직원 인사평가항목에 반영/평가		
물리적 보안	7.1 물리적 보호구역	(정보시스템이 있는) 통제구역 출입통로는		
		우회경로가 없도록 설정	출입구외부에 접견/물품 입출하구역 설치 → 불필요인원, 자산출입 최소화	
	7.2 시스템 보호	3개월평균 순간사용전력의 130%를 최소 20분 이상 공급 ex) 무정전전원장치(UPS), 비상발전기 등	(보호구역내 온습도,화재,수해,전압 등을) 〈자동화시스템〉으로 모니터링/ 대응	
		보호설비 주기적 점검 → 월 1회 책임자에게 결과보고		
		정전대비 비상발전기 부하 테스트		
		반기 1회 이상 수행	월 1회 이상, 부하테스트 연1회이상	
		보호구역내 출입자/자산 모니터링을 위해 CCTV 설치 →영상저장관리 [CCTV영상 식별수준] 실내 : 30만화소이상 실외 : 저조도환경대응, 100만화소 이상으로 주/야간영상 모두 보관	비정상행위발생시 자동경보시스템 구축 (발생위치, 로그, 사용자/영상정보 등) →관리자 즉각인지 / 대응	
		모든 보호구역에 시스템적으로 출입로그 남기는 잠금장치 설치 ex) 지문인식, 카드리더기 등		
		출입자현황 & 권한적정성 주기적검토 ex) 출입통제시스템 출입자권한/ 출입이력, 임시방문자 현황, CCTV 이상징후 등		
		월1회 이상 검토	주1회 이상 검토	
	7.3 사무실 보안	개인 PC 설정을 시스템적으로 관리 ex) 주기적 패스워드 변경, 자동화면보호기, 백신 등		
		정보보호준수사항 점검 매월 1회		
		(공용PC, 파일서버 사용시) 사용자별 이력확인을 위한 자동로그기록으로 책임추적성 확보		
		프린터 출력시 워터마크, 기록관리	출력물 본인 외 수령금지	Privacy-i

(뒷장에서 계속)

정보보호관리등급 세부평가기준

정보보호조치수준 (앞장에서 계속)

분야	항목	우수등급기준	최우수등급기준 (우수등급기준포함)	기술적 보호조치
시스템 개발보안	8.1 분석/ 설계보안관리	시스템 개발/변경시		
		사전영향평가로 보안요구사항 도출 → 설계반영	보안요구사항검토/승인절차 시스템화, 업무프로세스 반영	
	8.2 구현 / 이관보안	[구현단계] 〈소스점검 자동화툴〉로 코딩표준/시큐어코딩 준수여부 점검		
		[시험단계] 〈취약점점검도구 or 모의진단〉으로 기술적 보안취약점 점검 (개발조직 이외 조직이 수행)		
		개발/시험/운영 정보시스템간 상호네트워크 분리		
		정보시스템 개발관련 문서(계획서, 요구사항, 설계서, 각종도식자료), 소스프로그램현황, 변경이력 통제관리시스템 구축		
		운영데이터 복제/사용여부 매일 모니터링 → CSO결과보고		
	8.3 외주개발보안	외주개발업체 대상 보안요구사항		
		SLA(Service Level Agreement)로 협의	준수기준계량화→ 개발완료 후 인수시 활용	
암호통제	9.1정책	중요정보 명확히 정의, 저장/전송시 별도 암호화절차 수립		[서버 파일암호화] Server-i [PC 데이터암호화] Privacy-i
	9.2 키 관리	암호화함수와 키 분리보관	〈키관리시스템〉으로 암호키 생성/이용/폐기	
접근통제	10.1 권한관리	〈자동화 계정/접근권한 관리시스템〉으로 접근권한 통합등록, 변경, 삭제 → 사용현황 실시간 모니터링	협력사, 임시직 등 외부사용자 대상으로 구현	[DB] DB-i [WAS] was-i [SAP] App-i
		권한(메뉴별 or 개인별) 적정성 주기적 검토 일반권한 (분기별 1회) , 관리자권한/특수권한 (매월 1회)		
	10.2 인증 / 식별	사용자인증을 위해 〈접근제어시스템〉 구축 →패스워드 외 추가인증적용		
	10.3 접근통제 영역관리	(개인정보포함) DB서버와 일반서버 간 네트워크분리		
		(개인정보포함) DB는 테이블별로 접근권한 부여		[DB] DB-i [WAS] was-i [SAP] App-i
		DB관리자 권한범위 정의		
		월1회 이상 검토	주1회 이상 검토	
		업무용 모바일기기(스마트폰, 태블릿PC 등) 통제		SMART-i
		사전등록&관리절차 시행	통제프로그램 이용	
		모든 임직원대상 유해사이트접속차단, 접속현황 로깅		[세이프브라우징] WebKeeper™
		개인정보취급자/주요권한자 (서버 / DB 운영자/관리자, 개발자 등) PC의 인터넷 접속차단	· 차단PC/인터넷PC간 직접 전송금지 · 자료연계시스템 이용시 임계치설정& 주기적모니터링	

(뒷장에서 계속)

정보보호관리등급 세부평가기준

정보보호조치수준 (앞장에서 계속)

<table>
<tr><th>분야</th><th>항목</th><th>우수등급기준</th><th>최우수등급기준 (우수등급기준포함)</th><th>기술적 보호조치</th></tr>
<tr><td rowspan="15">운영보안</td><td>11.1
운영절차/
변경관리</td><td>운영절차(or 매뉴얼) 반기별 1회 이상 점검
→ 필요시 업데이트</td><td colspan="2">전과정 자동화시스템으로 관리
계획(공급/변경계획) → 도입(구매요청, 오더, 수령, 설치)
→운영(자산추적,보고,실사) → 폐기(매각,분실,폐기,기부)</td></tr>
<tr><td rowspan="14">11.2
시스템 및
서비스
운영보안</td><td colspan="3">정보시스템인수시 〈인수기준적합여부테스트(보안성검토 포함)〉 책임자지정 → CSO 승인</td></tr>
<tr><td>〈공식보안절차〉에 따라 시스템을 통해
〈방화벽정책등록, 변경, 삭제〉상시이력 조회</td><td colspan="2">모든 시스템 정책 등록,변경,삭제를
〈접근제어목록〉기반 공식절차로
시스템에서 운영/조회</td><td>[DB] DB-i
[WAS] was-i
[SAP] App-i</td></tr>
<tr><td colspan="3">보안시스템정책 타당성/변경이력 검토 월 1회 이상 → 검토결과 책임자 보고</td></tr>
<tr><td>〈장애이력 관리시스템〉으로
장애재발방지</td><td colspan="2">최고등급장애시
· CEO, CSO 가 실시간확인(SMS, Email 등)
· 대쉬보드로 장애현황 제공</td></tr>
<tr><td colspan="3">내부 네트워크접근을 위해 VPN이용시 PW 외 공인인증서, OTP 등 추가인증 사용</td></tr>
<tr><td colspan="3">VPN으로 접근시 단말(PC, 노트북 등) 보안수준 설정
ex) 개인방화벽, 인터넷차단, 다운로드 제한 등</td></tr>
<tr><td>통제구역에서 내외부 무선AP 를 통한
비인가 무선네트워크 접근통제</td><td colspan="2">통제구역에서 모든 미승인 무선접속통제
ex) 테더링, Wibro, 핫스팟 등</td></tr>
<tr><td colspan="3">공개서버 내 개인정보 등 중요정보 노출 여부를</td><td rowspan="2">[서버]
Server-i
[홈페이지]
WEB Privacy</td></tr>
<tr><td>월 1회 이상 점검 →CSO 보고</td><td colspan="2">상시점검시스템 운영</td></tr>
<tr><td colspan="3">· 백업대상별 백업복구 목표시간 (RTO, Recovery Time Objective)과
복구목표시점 (RPO, Recovery Point Objective) 정의
· RTO 적정여부확인을 위해 주요시스템 대상 복구테스트 연 1회 이상</td></tr>
<tr><td colspan="3">· 취약점전수점검 반기1회 이상, 취약점검결과조치율 98%이상
· 웹 취약점점검시 OWASP TOP 10 항목 모두 포함
· 취약점점검&모의침투테스트 주기적수행 →CSO 결과보고</td></tr>
<tr><td>· 취약점점검(분기1회 이상)
· 모의침투테스트(반기 1회 이상)</td><td colspan="2">· 취약점점검(격월)
· 모의 침투테스트(분기 1회 이상)</td></tr>
<tr><td>11.3
전자거래 및
전송보안</td><td colspan="3">타기관 or 기업간 정보전송시 보안요구사항 정의
→ 분기별 1회 이상 점검 → 문제점은 즉시 보안대책 적용</td></tr>
<tr><td rowspan="2">11.4
매체보안
(주요직무자
PC)</td><td>· 〈저장매체 통제시스템〉으로
사용내역 기록 / 모니터링
· 외장하드, CD, DVD 금지</td><td colspan="2">〈매체통제 우회시도〉
ex) 하드웨어분리 원천차단체계 적용,
HDD암호화, 가상장치인터페이스(VDI)</td><td rowspan="2">Privacy-i</td></tr>
<tr><td colspan="3">저장매체 사용로그 월1회 이상 점검→CSO에 보고</td></tr>
<tr><td>11.5
악성코드
(PC, 중요정보,
정보보호
시스템)</td><td>〈악성코드 실시간확인시스템〉 구축
ex) 백신 임의삭제/설정변경 금지,
백신 미설치시 네트워크 접근차단</td><td colspan="2">〈신종악성코드 신속탐지/대응체계〉 구축
ex) APT 대응체계, 좀비PC 탐지, 이상트래픽 분석</td><td>[세이프브라우징]
WebKeeper™</td></tr>
<tr><td colspan="3">〈중앙백신서버〉로
① 백신엔진 자동업데이트(무결성확인포함) ② 악성코드 월 1회이상 점검→CSO보고</td></tr>
</table>

(뒷장에서 계속)

정보보호관리등급 세부평가기준

정보보호조치수준 (앞장에서 계속)

분야	항목	우수등급기준	최우수등급기준 (우수등급기준포함)	기술적 보호조치
운영보안	11.6 로그관리 / 모니터링 (정보보호 시스템)	〈시각동기화서버〉로 모든 정보/정보보호시스템 표준시각동기화		
		〈중앙집중식로그수집시스템〉으로 로그수집	〈수집로그상시분석시스템〉 운영, 로그무결성 보장기능포함 ex) 타임스탬프, WORM디스크 등 로그위변조 방지기능	WORM 디스크
		〈통합모니터링시스템〉으로 24시간 모니터링 → 〈이상징후탐지 /보고체계〉로 신속대응	사용자~네트워크관문까지 모든 로그(빅데이터) 분석능력 확보 → 〈실시간 보안위협모니터링〉으로 위협탐지/차단 ex) · 네트워크기반 보안장비로그, · 서버/PC내 보안 S/W 로그 실시간수집 /분석 · 시나리오기반 외부침해/내부정보유출 탐지	DLP+Center DB방화벽, 엔드포인트DLP, 네트워크DLP 데이터 통합관리 [3년치로그 1분내검색] Mail-i BIGDATA
		〈침해시도 이상징후〉탐지시 즉시 경고, 대응 (알람, SMS 등)	〈침해시도이상징후〉를 전담인력이 24시간 모니터링	
		〈침해시도 모니터링 전담조직〉 구성	(전담조직 내) 침해시도 모니터링인력, 침해분석/대응인력 포함	
침해사고 관리	12.1 절차/체계	〈침해사고 대응조직〉 (CERT, Computer Emergency Response Team) 구축		Privacy consulting
	12.2 대응/복구	〈침해사고대응훈련〉 반기 1회이상 →CSO보고 · 유형별시나리오작성 ex) APT,해킹,개인정보유출 대응시나리오 · 모든 관련조직 참여 ex) 정보보호, IT운영/개발, 홍보, 법무, 총무	침해사고분석/법적증거능력 확보를 위한 〈포렌식절차/방법〉수립	
IT 재해복구	13.1 체계구축	업무영향분석(BIA)을 통해 〈정보자산범위〉 명확화 →복구목표시간 · 대책 구체적정의	IT 재해복구시설 확보, 복구목표시점을 준수하여 복구 ex) HW, 전력, 네트워크	
	13.2 대책구현	핵심 IT서비스/시스템 대상 〈복구목표시간준수여부확인테스트〉 모의훈련 수준으로 반기 1회 이상	(현장조치 대응능력을 평가하는) 〈IT재해복구훈련〉 실제수준으로 연 1회 이상	

발송일
2014. 08

2014년 8월 17일

정보통신망법 적용사업자 (통신/민간사업자) 기보유 주민번호 파기

2014.8.18일부터 법적근거가 없는 주민번호를 파기하지 않고 불법보유시 어떻게 되는가?

주민번호를 보유할 수 있는 경우 정보통신망법 23조의2

01	02	03
방통위지정 본인확인기관일 경우	법령에 수집/이용 근거가 있는 경우	방통위가 주민번호 수집/이용을 허용/고시한 경우

(유출되지 않더라도) 주민번호 미파기에 대하여 과태료/형사처벌

〈주민번호수집금지〉 규정위반으로 해석시
정보통신망법 제76조1항2호

과태료 3,000 만원 이하

〈목적달성 or 유효기간 끝난 개인정보 미파기〉로 해석시
정보통신망법 제73조 1의2호

형사처벌 2년 징역 or 2천만원 벌금 이하

주민번호 유출시 [고의/중과실] 해당확률 높음 : 손해배상+형사처벌+과징금

피해고객이 유리한 방식 선택

고객의 피해입증이 불가한 경우

법정손해배상

1인당 **최대 300만원**

정보통신망법 제32조의 2

고객의 피해입증이 가능한 경우

징벌적손해배상

1인당 **피해액의 3배까지**

국무총리실 범정부TF [개인정보보호 정상화대책]

정보통신망법고시 〈기술적,관리적 보호조치〉를 하지 않아 개인정보유출시

형사처벌

2년징역 or 1천만원벌금
→ **2년 징역 or 2천만원 벌금** 이하

정보통신망법 제73조 1호

과징금

매출의 1%까지
→ 위반행위관련 **매출의 3%**까지

정보통신망법 제64조의3 1항 6호

발송일
2013. 02

2013.2.18 개정정보통신망법고시 시행③

[ISMS(정보보호관리체계)인증]에 대한 고시

원문보기

· ISMS인증 의무대상자는 누구인가?
1. 서울, 부산, 인천, 대구, 광주, 대전, 울산에서 정보통신망서비스를 제공하는 기간통신사업자 or
2. 전년 매출 100억원 이상 or 전년말기준 3개월간 일평균 이용자수 100만명 이상인 정보통신사업자
(집적정보통신시설재판매업자 포함) or
3. 집적정보통신시설사업자

· 전과 무엇이 달라졌나? 위 대상자에 한해 권고사항에서 의무사항이 되었음

· ISMS인증은 누가 심사하는가? 한국인터넷진흥원(KISA)

· 인증 절차는 어떻게 되는가?
(인증기준에 부합하는) 정보보호관리체계를 구축하고 최소 2개월 이상 운영후 인증신청

ISMS (정보보호관리체계) 인증기준 중 기술적보호조치 관련 항목

정보자산분류

항목	내용	기술적 보호조치
4.1.1 정보자산 식별	분류기준 수립, 정보보호관리체계 범위 내 모든 정보자산을 식별하여 목록으로 관리	개인정보자산식별 Privacy-i
4.1.2 정보자산별 책임할당	식별된 정보자산에 대한 책임자 / 관리자 지정	
4.2.1 보안등급과 취급	정보자산에 보안등급 부여	

시스템 개발보안

항목	내용	기술적 보호조치
8.1.1 보안요구사항	시스템 개발 / 변경시 보안요구사항 명확히 정의 후 적용	
8.1.2 인증/암호화	· 사용자인증에 있어 보안요구사항 고려 · 정보취급과정에서 무결성, 기밀성, 법적 요구사항 고려	
8.1.3 보안로그	사용자인증, 권한변경, 중요정보 이용 / 유출 등에 대한 감사증적 확보	

(뒷장에서 계속)

시스템 개발보안 (앞장에서 계속)

항목	내용	기술적 보호조치
8.1.4 접근권한	업무목적 / 중요도에 따라 접근권한 부여	DB접근권한통제 DB-i
8.2.1 구현, 시험	안전한 코딩으로 시스템구현, 적용여부테스트수행, 취약성 노출여부 점검 후 대책수립	
8.2.2 개발/운영환경분리	비인가접근, 변경위험 감소를 위해 테스트시스템과 운영시스템 분리	
8.2.3 운영환경이관	통제된 절차에 따른 운영환경 이관, 실행코드는 테스트와 사용자인수후 실행	
8.2.4 테스트데이터보안	유출방지를 위해 테스트데이터에 대한 생성, 이용, 파기, 기술적 보호조치에 관한 절차 수립	
8.2.5 소스프로그램보안	인가자만 소스프로그램에 접근하도록 통제절차 수립, 이행, 소스프로그램은 운영환경에 보관하지 않음	
8.3.1 외주개발보안	외주위탁시 보안요구사항을 계약서에 명시, 이행여부 관리·감독	

암호통제

항목	내용	기술적 보호조치
9.1.1 암호정책 수립	암호화대상, 강도, 사용, 키관리에 대한 정책 수립, 이행	
9.2.1 암호키 생성/이용	암호키 생성, 이용, 보관, 배포, 파기에 관한 절차 수립, 복구방안 마련	

접근통제 (앞장에서 계속)

항목	내용	기술적 보호조치
10.1.1 접근통제정책 수립	비인가자의 접근통제 영역 / 범위, 규칙, 방법 등을 포함한 정책 수립	[DB방화벽] DB-i
10.2.1 사용자등록 및 권한부여	공식적사용자등록 / 해지절차 수립, 사용자 접근권한 최소한으로 부여	
10.2.2 관리자 및 특수권한관리	특수목적 계정/권한을 식별하고 별도통제	
10.2.3 접근권한 검토	접근권한 부여, 이용, 변경의 적정성 여부를 정기적으로 점검	
10.3.1 사용자인증	사용자인증, 로그인횟수 제한, 불법로그인 시도시 경고 등 시스템 접근통제	
10.3.2 사용자식별	사용자 구분을 위한 식별자할당·추측가능한 식별자제한, 식별자 공유시 승인절차	
10.3.3 사용자 패스워드	패스워드 관리절차 수립·이행·관리자 패스워드는 별도관리	

(뒷장에서 계속)

접근통제 (앞장에서 계속)

항목	내용	기술적 보호조치
10.3.4 외부이용자 패스워드 관리	외부이용자대상 패스워드 관리절차 마련 후 공지	
10.4.1 네트워크접근	네트워크접근통제리스트, 식별자관리절차수립, 서비스/사용자그룹/서비스자산중요도에 따라 내외부 네트워크 분리	
10.4.2 서버접근	서버별로 접근허용사용자/ 접근제한방식/안전한 접근수단 등 정의 후 적용	
10.4.3 응용프로그램 접근	응용프로그램 접근권한 제한, 불필요한 중요정보 노출 최소화	was-i
10.4.4 데이터베이스접근	· 데이터베이스 접근허용 응용프로그램/사용자 직무 명확히 규정 후 접근통제정책 수립 · 사용자접근내역 기록하고 타당성을 정기적으로 검토	DB-i
10.4.5 모바일기기 접근	모바일기기인증승인/접근범위/보안설정/오남용모니터링 등 접근통제 대책 수립	
10.4.6 인터넷 접속	· 주요직무자의 인터넷접속서비스(P2P,웹메일,웹하드,메신저 등)를 제한 · 인터넷접속은 침입차단시스템으로 통제 / 접속내역 모니터링	Mail-i WebKeeper

운영보안

항목	내용	기술적 보호조치
11.1.1 운영절차 수립	정보시스템의 동작, 문제시 재동작/복구, 오류처리 등 〈시스템 운영 절차〉 수립	
11.1.2 변경관리	관련자산 변경내역 관리절차 수립, 변경 전 성능 / 보안에 미치는 영향분석	
11.2.1 정보시스템 인수	시스템도입 or 개선시 필수 보안요구사항 포함한 인수기준 수립 후 인수 전 기준적합성 검토	
11.2.2 보안시스템 운영	시스템 유형별로 관리자 지정, 최신정책 업데이트, 룰셋변경, 이벤트모니터링 등의 운영절차 수립 후 현황관리	
11.2.3 성능 / 용량관리	시스템/서비스 가용성보장을 위해 성능/용량요구사항을 정의하고 현황을 지속적으로 모니터링	
11.2.4 장애관리	장애발생시 대응을 위한 탐지, 기록, 분석, 복구, 보고절차 수립	
11.2.5 원격운영 관리	· 내부네트워크로 시스템관리시 특정단말에서만 접근 허용 · 외부네트워크로 관리금지, 부득이한 경우 보호대책(책임자승인, 인증, 암호화, 보안 등)수립	

(뒷장에서 계속)

운영보안 (앞장에서 계속)

항목	내용	기술적 보호조치
11.2.6 스마트워크 보안	원격업무수행시 관리.기술적 보호대책 수립/이행	
11.2.7 무선네트워크 보안	무선인터넷 사용시 네트워크구간에 대한 보안강화대책(사용자인증, 송수신데이터암호화) 수립	
11.2.8 공개서버 보안	웹사이트 등에 정보공개시 수집,저장,공개에 따른 허가/게시절차 수립, 공개서버 보호대책 수립	was-i
11.2.9 백업관리	백업대상/주기/방법 절차 수립, 사고발생시 복구관리	
11.2.10 취약점 점검	정기적으로 취약점점검을 수행하고 발견된 취약점을 조치	
11.3.1 전자거래 보안	전자거래서비스 제공시 사용자인증, 암호화, 부인방지 등 보호대책수립, 외부시스템 연계시 안전성 점검	
11.3.2 정보전송정책수립 및 협약체결	타조직에 중요정보 전송시 정책수립 후, 합의를 통해 관리책임/전송기술표준/보호조치 포함 협약서 작성	
11.4.1 정보시스템저장 매체관리	하드디스크, 스토리지, 테이프 등 저장매체 폐기/재사용절차수립, 중요정보는 완전삭제	
11.4.2 휴대용 저장매체 관리	외장하드,USB, CD 등 휴대용저장매체 취급/보관/폐기/재사용절차 수립, 매체를 통한 악성코드감염방지 대책 마련	
11.5.1 악성코드통제	악성코드 예방/탐지/대응 등의 보호대책 수립	WebKeeper
11.5.2 패치관리	침해사고예방을 위해 최신패치를 정기적으로 적용하고 시스템에 미치는 영향 분석	
11.6.1 시각동기화	정확성과 법적인 효력을 위해 정보시스템 시각을 공식 표준시각으로 정확하게 동기화	
11.6.2 로그기록/보존	기록해야 할 로그유형을 정의하여 일정기간 보존하고 주기적으로 검토	DB-i Mail-i
11.6.3 접근/사용모니터링	중요정보, 정보시스템, 응용프로그램, 네트워크장비에 대한 접근이 허용된 범위인지 주기적 확인	
11.6.4 침해시도모니터링	외부로부터의 침해시도 모니터링 위한 체계/절차 수립	

발송일
2013. 02

2013. 2.18 개정정보통신망법고시 시행②

[정보보호사전점검]에 관한 고시 원문보기

· [정보보호사전점검]은 사업자가 자체적으로 하는가? 아니면 전문기관이 하는 것인가?
자체적으로 할 수도 있고 (방통위 지정) 사전점검수행기관에게 받을 수도 있음
자체적으로 할 경우에는 자격요건을 갖춘 직원이 정보보호사전점검교육을 받은 후 수행팀을 꾸려야 함

· [정보보호사전점검]은 의무인가? 권고인가? 대상은 누구인가?
권고이며 권고대상은
① 방통위 인 · 허가/등록 · 신고대상인 정보통신서비스/전기통신사업 중 정보시스템구축비 5억이상
(HW,SW 단순구입비 제외)
② 방통위가 사업비를 지원하는 시범서비스/사업

· [정보보호사전점검]을 하면 어떤 이익이 있는가? 방통위 인/허가, 등록/신고에 있어 가점 부여

· [정보보호사전점검]은 언제 하는 것인가? 정보통신망 구축 or 서비스 개시 이전에 실시

· [정보보호사전점검] 대상은 어디인가?
사업 or 서비스를 구성하는 HW, SW, 네트워크 등의 유 · 무형 설비 및 시설

[정보보호사전점검에 관한 고시] 보기 (1)

· 〈대상자〉 사전점검을 받는 사업자
· 〈점검팀〉 자격요건을 갖춘 내, 외부인력으로 구성한 사전점검 수행팀

조항	내용
19조 (준비)	〈대상자〉는 〈점검팀〉을 구성, [사전점검수행계획서] 작성
20조 (설계검토)	〈점검팀〉은 아래 순서로 설계검토 ① 서비스정의 ② 서비스 구조분석 ③ 보호자산식별 ④ 위협 분석 ⑤ 취약점 분석 ⑥ 위험 분석 ⑦ 위협 시나리오 도출 ⑧ [보호대책] 도출
21조(보호대책적용)	〈대상자〉는 [보호대책]을 적용

[정보보호사전점검에 관한 고시] 보기 (2)

22조 (보호대책구현현황 점검 / 시험)	〈점검팀〉은 [보호대책] 구현현황을 점검 ① 실제 구현현황 파악 ② 위협시나리오에 따라 모의해킹/침투시험 실시
23조 (결과정리)	〈점검팀〉은 [사전점검결과보고서] 작성, 대상자에게 제출
24조 (결과처리)	① 대상자는 (사전점검결과에 따라 적용 않은 보호대책이 있을 경우) **보호조치계획**을 수립, 반영 ② 심각한 위험이 발견된 경우 보호대책을 구현한 이후에 통신망 or 서비스를 운영

설계검토단계 중 보호자산식별은 어떻게 하는가?

정보통신망/서비스로 접근가능한 정보를 모두 검출, 식별, 분류

개인정보는 Privacy-i로 검출, 식별

〈평가요소에 따라 등급부여〉

평가요소	평가등급	평가점수	평가기준 설명
기밀성 (Confidentiality)	H	3	매우 민감한 정보이므로 업무관련 책임자만 접근가능
	M	2	민감한 정보이므로 내부담당자, 책임자 등 일부 허가된 직원만 접근가능
	L	1	민감한 정보는 아니나 내부인만 접근가능
무결성 (Integrity)	H	3	정보의 무결성 손상시 서비스 제공에 치명적인 영향을 주며, 주요업무/회사기능에 마비를 초래할 수 있음
	M	2	정보의 무결성손상시 서비스 제공에 중대한 영향을 줌
	L	1	정보의 무결성 손상시 서비스 제공에 경미한 영향을 주지만, 충분히 해결할 수 있음
가용성 (Availability)	H	3	24시간 항상 가동이 필요하며 중단되어서는 안 됨
	M	2	근무시간 중에는 항상 접근 가능해야 함
	L	1	근무시간 중에 50%이상 사용 가능해야하고 접근 가능해야 함

발송일
2013. 02

2012.2.18 개정정보통신망법고시 시행①

[정보보호조치]에 관한 지침 원문보기

· 무엇이 어떻게 바뀐 것인가?

안전진단제도가 폐지되면서 기존 [정보보호조치 및 안전진단 방법 · 절차 · 수수료에 관한 지침]을 [정보보호조치에 관한 지침]으로 변경

· 법적 근거는 무엇인가? 개정정보통신망법 제45조

제45조 (정보통신망의 안정성 확보 등)

① 정보통신서비스 제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다.

② 방송통신위원회는 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치에 관한 지침 (이하 "정보보호지침"이라 한다)을 정하여 고시하고 정보통신서비스 제공자에게 이를 지키도록 권고할 수 있다 〈개정 2012.2.17〉

③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다.

1. 정당한 권한이 없는 자가 정보통신망에 접근/침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치/운영 등 기술적/물리적 보호조치
2. 정보의 불법 유출/변조/삭제 등을 방지하기 위한 기술적 보호조치
3. 정보통신망의 지속적 이용가능상태를 확보하기 위한 기술적/물리적 보호조치
4. 정보통신망의 안정, 정보보호를 위한 인력/조직/경비의 확보 및 관련 계획수립 등 관리적 보호조치

신설규정들

CISO(정보보호최고책임자)를 이사 이상 상근임원으로 선임

관련 법, 규제, 계약, 정책, 기술상의 요구사항을 정의, 문서화, 준수

IT예산의 5% 이상을 보안예산으로 사용

[정보보호사전점검제] 정보통신망 신규구축, 제공시 계획, 설계, 구현, 테스트 단계에서 정보보호 고려

정보보호투자/인력현황, 관련인증 등을 홈페이지 등에 공개

정보통신설비 및 시설 목록 (용도/위치 포함) 작성 네트워크와 분리된 환경에서 안전하게 관리

관리용단말은 인터넷과 격리하여 외부접속차단

주민번호, 신용카드번호, 계좌번호, 정보자산현황을 안전한 알고리즘으로 암호화저장

관리적, 기술적, 물리적 보호조치 57개 규정 원문보기

관리적 보호조치

구분	세부조치사항
1.1.1. 조직 구성	· 최고책임자, 관리자, 담당자로 구성된 정보보호조직운영
변경 1.1.2. CSO 지정	· 이사 이상 상근임원으로 지정
1.1.3. 역할	· CSO는 총괄지휘, 관리자는 실무총괄/관리, 담당자는 분야별 실무담당
1.2.1. 방침	· 정보보호목표, 범위, 책임 등을 포함한 [정보보호방침] 수립 신설 · 정보통신서비스 관련 모든 법, 규제, 계약, 정책, 기술상의 요구사항을 정의, 문서화, 준수
1.2.2. 실행계획	· [정보보호방침]을 토대로 매년 [정보보호실행계획] 수립 (예산, 일정 포함) · 최고경영층이 [정보보호실행계획] 승인, CSO가 반기마다 추진상황 점검
1.2.3. 실무지침	· 정보통신설비 및 시설에 대한 보호조치 시행방법/절차 등을 규정한 [정보보호실무지침] 마련 · CSO가 실무지침을 승인, 관련 법/제도, 설비의 교체 등 변경발생경우 보완
신설 1.2.4. 사전점검	· 정보통신망 신규구축, 제공시 계획, 설계, 구현, 테스트 단계에서 정보보호 고려
1.3.1. 내부인력	· 전보/퇴직시 즉시 접근권한 제거 · 인식 제고를 위한 홍보실시 및 정보보호업무종사자 대상 정기적 교육
1.3.2. 외부인력	· 외부인력에 보안서약 청구
1.3.3. 위탁운영	· 전산업무 외부위탁시 보안계약서 및 서비스 수준협약 등에 '정보보호에 관한 위탁업체의 책임범위', '위탁업무중단에 따른 비상대책' 등을 반영
1.4.1. 정보보호정보 제공	· 이용자에게 침해사고 예/경보, 보안취약점, 계정/비밀번호 관리방안 등 정보 지속제공
신설 1.4.2. 정보보호 현황공개	· 정보보호투자/인력현황, 관련인증 등을 홈페이지 등에 공개
1.5.1. 침해사고 대응계획의 수립 및 이행	· 침해사고정의/범위, 대응체계(보고/조치체계), 대응방법/절차, 복구방법/ 절차, 증거자료 수집/ 보관 등을 포함한 [침해사고대응계획] 마련/시행
1.6.1 보호조치 자체점검	· 정보보호관리자는 매년 본 지침 및 [정보보호실무지침]을 따라 자체점검
1.7.1. 정보통신설비 및 시설현황관리	· 정보통신망구성도 마련 및 변경시 보완/관리 · 정보통신설비 및 시설목록(용도/위치 포함) 작성/ 네트워크와 분리된 환경에서 안전하게 관리
신설 1.8.1. 정보보호 투자계획 수립 및 이행	· 위험관리에 기반한 적정수준(정보기술부문예산의 5%이상)의 예산편성 및 집행

관리적, 기술적, 물리적 보호조치 57개 규정

기술적 보호조치

구분		세부조치사항	기술적보호조치
2.1 네트워크 보안	2.1.1. 트래픽모니터링	· 네트워크모니터링 도구를 이용하여 백본망, 주요노드, 외부망과 연계되는 주요회선의 트래픽 소통량을 24시간 모니터링	
	2.1.2. 무선서비스	· 무선랜/ 무선인터넷서비스 제공시 사용자인증, 데이터암호화 등 보안조치마련	
	2.1.3. 정보보호시스템 설치 · 운영	· 외부망연계구간에 침입차단/침입탐지 등 정보보호시스템 설치/운영	
	신설 2.1.4. 정보보호를 위한 모니터링	· 허용범위 안에서 중요 시스템/네트워크를 사용, 접근하는지 확인하기 위한 모니터링 시스템 구축 or 위탁운영을 통하여 침해사고 탐지/대응체계운영	
2.2 정보통신설비 보안	2.2.1. 웹서버	· 외부서비스 웹서버는 단독서버로 운영 및 DMZ에 설치	
	2.2.2. DNS서버	· 과부하 대비 부하분산대책 마련 및 설정파일 백업 실시	
	2.2.3. DHCP서버	· 과부하대비 부하분산대책마련 및 설정파일 백업실시 · IP할당상황 등에 대한 로그기록 유지/관리	
	2.2.4. DB서버	· 내부망에 설치 · 외부망에서 직접 접속할 수 없도록 네트워크 구성	
	2.2.5. 라우터/스위치	· ACL 등 접근제어기능 적용설비 사용`	

(뒷장에서 계속)

관리적, 기술적, 물리적 보호조치 57개 규정

기술적 보호조치 (앞장에서 계속)

구분	세부조치사항	기술적 보호조치

관리적, 기술적, 물리적 보호조치 57개 규정

물리적 보호조치

구분	세부조치사항
3.1.1. 정보통신시설의 출입/접근 통제	· 비인가자가 출입할 수 없도록 잠금장치 설치 · 출입기록을 1개월 이상 유지/보관
3.2.1. 백업설비 및 시설 설치/운영	· 백업설비 및 시설 설치/운영

발송일
2012. 08

2012.8.18 개정정보통신망법 시행②

개인정보취급자 PC [논리적 or 물리적망분리] 실시

· 망분리의 법적 근거는 무엇인가?
› 개정 정보통신망법 제29조 2항, 시행령 제15조의 2

· 망분리규정은 어느 사업자에게 적용되는가?
› 전년말 기준 직전 3개월간 평균 100만명 이상 개인정보 보유 사업자 or
정보통신서비스부문 전년 매출액 100억원 이상 사업자
*사이트나 서비스 기준이 아니라 사업자기준으로 측정함
예) 사업자 A가 웹사이트 4개를 운영할 경우 다 합쳐서 100만명, 100억원이 넘으면 망분리 적용대상임

· 사내 개인정보취급자 PC 전체에 망분리를 적용해야 하는가?
› 개인정보취급자 PC 전체가 아님
데이터베이스에 접근해서 개인정보를 (단순조회가 아니라)
다운로드 or 삭제 or 파기 or 데이터베이스 접근권한설정을 바꿀 수 있는 개인정보취급자 PC에 적용

· 물리적, 논리적 망분리 모두 가능한가?
› 모두 허용

· 지금 망분리를 구현하지 않으면 법적처벌을 받는가?
› 개인정보의 기술적 관리적 보호조치의 망분리규정은 2013년 2월 18일부터 시행되며
미이행으로 인한 유출시 2년 징역 1천만원 이하 벌금에 처해짐

정보통신망법개정안 | 정보통신망법시행령개정안 | 개정정보통신망법고시

60p [개인정보의 기술적 관리적 보호조치 기준] 규정 보기
정보통신망법고시
[개인정보의 기술적 관리적 보호조치 기준] 내 망분리 규정보기

발송일
2012. 08

2013.8.18 개정정보통신망법 시행①

2012.8.18 부터 온라인 주민번호 신규수집금지
2014.8.17 까지 보유중인 주민번호 파기

온라인에서 주민번호 신규수집금지	보유 주민번호 파기
▶ 위반시 과태료 3천만원	▶ 2014년 8월 17일까지

· 주민번호수집은 언제부터 실제 금지되는가?
6개월간의 계도기간을 거쳐 2013년 2월 18일부터 처벌됨

· 주민번호를 수집/이용할 수 있는 경우는 무엇인가?
› 본인확인기관으로 지정받은 경우
› 다른 법에 주민번호 수집,이용이 명시되어 있을 경우
› 주민번호 수집,이용이 불가피한 사업자로 방통위가 고시하는 경우

· 이전에 보유중인 주민번호는 언제까지 파기해야 하는가?
› 2년 내(2014년 8월 17일까지) 파기해야 함

· 주민번호대체수단이란 무엇을 말하는가?
(방통위에서 본인확인기관을 지정할 예정으로) 본인확인기관은 주민번호의 기존역할을 대체하는 주민번호대체수단으로 본인확인정보, 연계정보, 중복가입확인정보 등을 제공함
ex) 아이핀, 공인인증서, 핸드폰인증 등으로 암호화된 주민번호 파생값

3단계에 걸쳐 2014년까지 주민번호 수집이용 완전 차단

1단계(2012년)
일 방문자 1만명 이상 웹사이트 우선적용

- 방통위가 조사,규정 적용예정
- 주민번호전환 지원센터를 통하여 사업자 지원예정

2단계(2013년)
모든 웹사이트 주민번호 수집이용 금지

- 실태조사, 무료 컨설팅진행
- 불법 주민번호수집 웹사이트 신고창구 운영

3단계(2014년)
영리목적 웹사이트 주민번호 수집이용 완전차단

- 주민번호 수집이용여부 상시점검
- 영리 웹사이트 대상 주민번호 DB삭제여부 점검 실시

주민번호 파기, 실제 어떻게 구현하는가?

이런 경우에는		이렇게 합니다	
사례 1	· 외부연계 없음 · DB에서 색인키, 참조키로 미사용 · 수집만 하고 활용하지 않음	소만사 Privacy-i 로 전사적 주민번호 검출, 현황분석, 유효기간 확인	사례 1 일괄삭제 (Privacy-i 활용)
사례 2	· 외부연계 없이 내부에서만 사용 · 주민번호 현황파악 후 일괄삭제를 즉시 할 수 없거나 어려운 경우		사례 2 주민번호를 다른내용으로 대체 (자체적방법사용)
사례 3	· 외부연계 활용시 · 재가입방지/블랙리스트 관리 등 이용자식별수단으로 활용하는 경우		사례 3 주민번호 대체수단도입 (아이핀등 공인된 방법 사용)

발송일
2010. 09

2010년11월15일

PIMS(개인정보 관리체계) 인증 시행

WHO	방송통신위원회가 한국인터넷진흥원을 인증기관으로 지정하여
TO WHOM	기업체 대상으로
WHAT	개인정보보호활동을 체계적, 지속적으로 수행하기 위한 3개 분야, 119개 통제사항, 325개 세부점검항목 제시, 만족할 경우 인증 부여
HOW	인증희망기업은 한국인터넷진흥원에 신청서 접수, 문서심사와 현장심사를 거침 (연 1회 사후관리심사 및 3년 후 갱신심사 실시)
WHEN	2010년 하반기 시범적으로 실시. 2011년부터 활성화

기업체가 PIMS인증을 획득할 경우 혜택은?

- 정보통신망법 시행기관인 방송통신위원회, 한국인터넷진흥원이 주관하는 개인정보보호 인증
- 정보통신망법, 개인정보보호법 등 법적 기준 준수가 주요건으로,
  획득시 기업이 법적규정을 준수하였음을 대외적으로 증명할 수 있음
- 획득 경우 개인정보보호 관련 과태료/과징금 감면,
  명백한 고의나 과실이 아닐 경우 형사처벌 감형 등의 혜택을 기대
- 고객에게 귀중한 개인정보를 보호하는 기업임을 증명할 수 있음

PIMS인증 심사항목 중 기술적 보호조치 부분 요약

항목	통제사항	통제내용	기술적 보호조치
접근통제	7.1.1 정책	취급자에 대한 접근통제정책 수립, 문서화	[DB] DB-i [WAS] was-i [SAP] App-i
	7.1.2 등록	공식적 개인정보취급자 등록 및 해지절차 마련	
	7.1.3 권한관리	접근권한을 최소인원에게 부여, 내역 기록관리	
	7.1.4 패스워드	패스워드 관리절차 수립 이행	
	7.1.5 접근권한	접근권한 정기적 점검	
	7.1.6 책임	개인정보처리시스템/패스워드관리책임지침 제공	
	7.1.7 네트워크	네트워크의 내/외부 연결통제 사용자 터미널과 컴퓨터 서비스간 물리적/논리적 경로통제 사용자인증, 고장진단포트 접근통제 등 네트워크 접근정책 수립이행	[네트워크DLP] Mail-i™
	7.1.8 운영체제	로그온절차, 인증, 터미널자동확인 등 운영체제 접근통제	
	7.1.9 응용프로그램	접근불허된 응용프로그램 대상 정보제공 제한 출력물은 허가된 위치에서만 출력	[엔드포인트DLP] Privacy-i
	7.1.10 DB 접근	데이터테이블 레벨에 따른 접근통제, 데이터 및 DB유틸리티 접근통제, 암호화 등으로 DB내 정보보호	[DB방화벽] DB-i
암호화	7.2.1 정책	암호화를 위한 문서화된 정책 수립	[서버 개인정보암호화] Server-i [PC 개인정보암호화] Privacy-i
	7.2.2 사용	암호정책에 따라 암호대상 개인정보 암호화 실시	
	7.2.3 키관리	암호키관리지침, 절차, 방법, 복구방안 마련	
변경관리 등 운영보안 유지대책	7.3.1 변경관리	〈개인정보처리시스템〉 관련 자산조사, 변경사항반영 공식절차 수립	
	7.3.2. 직무분리	시스템오용위험 감소를 위한 직무분리	
	7.3.3 개발/운영분리	개발, 테스트, 운영환경 분리	
	7.3.4 네트워크운영	직무분리, 접근권한통제, 원격접속설비 관리, 네트워크분리 등을 위한 책임/절차를 포함한 대책 수립	[네트워크DLP] Mail-i™
	7.3.5 인터넷 접속관리	인터넷접속통제정책 수립, 침입차단/ 탐지시스템 설치	
	7.3.6 원격운영관리	시스템관리는 내부 특정터미널에서만 하며 외부에서 네트워크를 통해 시스템을 관리할 때는 사용자 인증, 암호, 접근통제 기능을 설정	
	7.3.7 매체취급/보관	매체 취급 /보관절차 수립 운영	
	7.3.8 매체 폐기	매체 폐기지침 수립 운영	
	7.3.9 악성프로그램	악성프로그램 예방, 탐지, 대응대책 수립	[세이프브라우징] WebKeeper™
	7.3.10 이동컴퓨팅	휴대용정보통신기기 사용시, 개인정보보호대책수립	
	7.3.11 원격작업	원격작업시 물리적 논리적 보호 정책/절차마련	
	7.3.12 공개서버보안	웹서버로 개인정보처리시 공개서버에 대한 기술적, 물리적 보안대책 수립/운영	

(뒷장에서 계속)

PIMS 인증 심사항목 중 기술적 보호조치 부분 요약 (앞장에서 계속)

항목	통제사항	통제내용	기술적 보호조치
영향 평가	7.4.1 분석/설계보안	〈개인정보처리시스템〉 구매, 개선시 영향평가 수행	Privacy consulting
	7.4.2 구현/시험	〈개인정보처리시스템〉 보안요구사항 만족대책구현, 보안요구사항 시험 수행	
	7.4.3 운영환경 이행보안	개인정보운영프로그램 수정은 권한자만이 시행, 개인정보운영시스템은 실행코드만 보유	
	7.4.4 테스트데이터보안	테스트데이터는 중요정보 변경, 삭제시행, 완료후 삭제	
	7.4.5 소스프로그램	실제운영환경에 보관하지 않음. 운영시스템별로 관리자 지정, 접근통제절차 수립/이행	
	7.4.6 변경관리	〈개인정보처리시스템〉변경에 따른 위험최소화를 위하여 공식적 변경관리절차 수립	
	7.4.7 운영체제 변경시 검토	운영체제 변경시 시스템운영 및 보안에 미치는 영향분석, 검토	
	7.4.8 패키지 변경	정책/법 만족, 변경사항은 시험하고 문서화	
출력 복사	7.5.1 용도특정	개인정보출력시 용도특정, 출력항목 최소화	[엔드포인트DLP] Privacy-i
	7.5.2 기록/승인	이동식저장장치, 출력물 복사시 기록, 사전승인	
	7.6.1 마스킹	업무상 조회출력시, 개인정보 마스킹	[개인정보마스킹] DB-i Privacy-i

관리과정, 보호대책, 생명주기에서 주목할 항목

항목	통제사항	통제내용	기술적 보호조치
분류	3.1.1 조사	개인정보자산 조사, 중요도 결정	Privacy-i
	3.1.2 책임할당	개인정보자산별 책임소재 명확화	
	3.2.2 흐름분석	분류/식별된 개인정보 수집, 이용, 제공, 저장, 관리, 파기 등 흐름파악	
	3.2.3 보안등급	분류/식별된 개인정보에 보안등급 부여, 표시부착 등	

04
금융

발송일
2015. 05

2015년 4월 16일부터 시행중입니다

금융감독원
[전자금융감독규정 시행세칙] 일부개정안①

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] 제60조 (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, 외주관리 책임 구체화

신설 **[전자금융감독규정 시행세칙]** 제9조의2 (외부주문 등에 대한 기준)

① 규정 제60조 1항7호에 따라 감독원장이 정하는 **〈보안관리방안〉**은 〈별표 5-2〉와 같다

② 규정 제60조 1항14호에 따라 감독원장이 정하는 **〈(일일)중요점검사항〉**은 〈별표5-3〉과 같다

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	

외주단계별〈보안관리방안〉31개 항목

외주단계		금융회사의 보안관리방안	기술적 보호조치
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	
		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	[개인정보처리시스템 접근통제] (DB) DB-i (WAS) was-i (SAP) App-i
		26. 용역업체 PC는 인터넷연결 금지, 필요시 금융회사 통제하에 제한적 허용	
		27. 용역업체 사용 전산망에는 자료공유사이트(P2P, 웹하드 등) 접속 원천차단	[비업무사이트접속차단] WebKeeper™

[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	

발송일
2015. 05

2015년 4월 16일부터 시행중입니다

금융감독원
[전자금융감독규정 시행세칙] 일부개정안②

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] 제37조의5 (정보보호최고책임자의 업무)

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

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

신설 **[전자금융감독규정 시행세칙]** 시행세칙 제7조의3 (정보보호최고책임자의 업무)

규정 제37조의5에 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]

CISO가 CEO에게 보고해야하는 34개〈정보보안 점검항목〉

구분	내용	기술적 보호조치
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	

발송일
2014. 11

개인정보보호책임자는 CEO이기에

유출사고발생/법규위반시 CEO의 리스크 [금융기관] 편

금융기관 CEO의 위험

1. 금융기관 업무정지

2014. 6. 30 실시

금감원
[금융기관검사 및 제재에 관한 규정] 시행세칙 개정안

2. 금융기관 개인정보보호 책임자로 CEO 명시

2014.03.10 발표
금감원 [금융분야 개인정보유출 재발방지종합대책]

2014.02.14 발표
금감원 [자체점검체크리스트]

2013.11.23 시행
금융위 [전자금융거래법] 개정안

2013.11.23 발표
금융위 [금융전산보안강화 종합대책]

CEO가 대표하는 법인의 위험

1. 손해배상 소송 및 배상액 확대

2014.07.31 발표
[개인정보보호 정상화 종합대책]

징벌적 손해배상 | 법정 손해배상 도입

2014년
집단손해배상소송

기업측패소, 손해배상판결
(A사 1심 , B사 2심)

2. 브랜드가치 훼손

장기적, 치명적 피해

CEO 개인의 위험

3. CEO 해임가능

2014.07.31 발표
[개인정보보호 정상화 종합대책]

CEO에게 유출시
책임부과, 해임가능

2014.08.07 시행
[개인정보보호법 개정안]

법규위반시
CEO 징계권고

4. CEO 형사처벌 가능

양벌규정
(개인정보보호법74조) + 2014년 이후 시대적변화

유출/법규위반시 **CEO** 잘못으로 판단할 가능성 상승

CEO, 법인 모두 형사처벌 받을 가능성 상승

1. 금융기관 영업정지: 정보보호 소홀정도가 높을 경우

2014.06.30 시행
금융기관 검사 및 제제에 관한 규정 시행세칙 개정안

원인 / 미준수 정도	정보보호 소홀정도가 높을 경우		정보보호 소홀정도가 낮을 경우	
	금융기관	임직원	금융기관	임직원
중대	업무정지	정직이상	업무정지	감봉
보통	기관경고	감봉	기관경고	견책
경미	기관주의	견책	-	-

정보보호 소홀 판단근거는
금감원
[기술적·물리적·관리적 보안대책]
준수여부

금감원 [기술적·물리적·관리적 보안대책]

근거조항) 신용정보법 시행령 제16조 1항

기술적 · 물리적 보안대책

조	내용	기술적 보호조치
1조 접근통제	① 〈개인신용정보처리시스템〉 접근권한은 필요최소인원에게 부여 ② 취급자 변경시 지체없이 〈개인신용정보처리시스템〉 접근권한변경, 말소 ③ 권한부여, 변경, 말소내역 기록, 최소 3년보관	[DB 접근권한관리, 기록] DB-i
	④ 〈개인신용정보처리시스템〉에 침입차단/침입탐지시스템 설치	[이상징후탐지] DB-i , was-i , App-i
	⑤ 패스워드 작성규칙 수립	
	⑥ 〈개인신용정보〉가 홈페이지, P2P, 공유설정 등으로 공개되지 않도록 〈개인신용정보처리시스템〉 및 취급자 PC 설정	[네트워크DLP] Mail-i [서버내 개인정보검출] Server-i
2조 접속기록 위변조방지	① 〈개인신용정보〉 접속기록 저장, 월 1회 이상 확인 · 감독 ② 〈개인신용정보처리시스템〉 접속기록 위변조방지	[개인정보 조회기록보관 및 위변조방지] DB-i , was-i , App-i
3조 개인신용정보 암호화	① 인증정보(패스워드, 생체정보)는 일방향 암호화저장 ② 〈개인신용정보〉 및 인증정보 송 · 수신시 암호화	
	③ 〈개인신용정보〉 PC저장 시 암호화	[PC내 개인정보암호화] Privacy-i
4조 컴퓨터 바이러스 방지	① 바이러스, 스파이웨어 등 악성프로그램 점검 · 치료를 위해 백신 설치 ② 백신 월1회이상 갱신 · 점검, 바이러스경보/업데이트시즉시 갱신 · 점검	
5조 출력복사시 보호조치	① 〈개인신용정보〉출력(인쇄, 화면표시, 파일생성 등)시 용도명확화, 출력항목 최소화 ② 〈개인신용정보〉 매체저장, 이메일 등 외부전송시 사전승인 ③ ① ②항준수에 필요한 내부시스템 구축	[파일생성방지] DB-i [엔드포인트DLP] Privacy-i [네트워크DLP] Mail-i

관리적 보안대책

조	내용	기술적 보호조치
1조 신용정보관리, 보호인	① 〈신용정보관리, 보호인〉 업무 1. 내부관리규정 제,개정 2. 고충처리 3. 임,직원 신용정보관리, 보호 4. 정보주체권리행사에 대한 이행여부점검 5. 임,직원 교육실시	
	② 〈신용정보관리, 보호인〉은 업무처리기록 3년보존, 점검결과 경영진 보고 및 업무처리절차에 반영	[개인정보 조회기록보관 및 위변조방지] DB-i
2조 개인신용정보 조회권한 구분	① 〈신용정보관리, 보호인〉은 〈개인신용정보〉 조회권한을 직급, 업무별로 차등부여	[조회권한관리] DB-i
	② 신용정보회사등은 〈개인신용정보〉 조회기록을 주기적점검, 점검결과 업무 반영	[접근기록관리] DB-i
	③ 〈신용정보관리, 보호인〉은 신용조회기록 정확성을 점검	
3조 제재기준	① 신용정보회사는 〈개인신용정보〉오, 남용자체제재기준 마련	

2. 개인정보보호 책임자로 금융기관 CEO 명시

(1) 2014.03.10, 범정부연합 (금융위,금감원, 안행부, 방통위,미래부,기재부) 발표 금융분야 개인정보유출재발방지 종합대책

2014년 금융권 유출사고 후 CEO 관심부족을 기존 문제점으로 명시

금융회사 CEO, 임원책임확대

핵심사항	현황 및 문제점	개선방안	기술적 보호조치
〈신용정보 관리·보호인〉 임원임명	·CEO관심부족 임원대상 개인정보보호 보고부족 ·법규준수를 위한 관리체계 미흡	·CEO 관리책임 명확화 ·신용정보관리·보호인을 임원으로 임명 ·신용정보관리·보호인은 CEO보고 월1회 이상, 이사회보고 연 1회 이상 신용정보법개정	Privacy consulting
CISO 책임강화	(보안과 상충하는) 타 IT직위와 겸직가능	·타 IT직위와 겸직불가 전자금융거래법개정	

CEO보고, CISO책임하에 정보보안관련 점검관리강화

핵심사항	현황 및 문제점	개선방안	기술적 보호조치
금감원 철저점검	〈내부통제규정〉이 실행단계에서 제대로 지켜지지 않음	[금융회사] ·자체 보안규정보완·구체화 ·규정준수여부를 CISO 책임하 매월 점검 (보안점검의 날 지정) ·취약점 즉시 보완 → CEO에게 결과보고 ·업무별·직급별 고객정보 접근권한 범위를 명확히 하는 '보안등급제' 추진 [금감원] ·법규준수여부 철저점검, 엄중 제재 ·불시점검 기동점검반 운영	DB방화벽 DB-i 접근권한통제 Privacy-i PC내 실태점검 Server-i 서버내 실태점검

〈금융분야 개인정보유출 재발방지 종합대책〉〈개인정보보호 정상화 종합대책〉 모두 CEO에게 보고 및 CEO책임강화 포함

2014.07.31 발표
개인정보보호정상화종합대책

유출사고 발생시 책임자로 CEO 명시

CPO대상 [CEO에 대한 보고의무] 부과
위반시 과태료 2천만원

CEO대상 [유출시 책임] 부과, [해임] 등 징계권고
시행중 개 신 개정예정 정

개 인정보보호법 신 용정보법 정 보통신망법

(뒷장에서 계속)

2. 개인정보보호 책임자로 금융기관 CEO 명시 (앞장에서 계속)

(2) 2014.02.14, 금융권 유출사고 이후 금융권 3,050개사 대상 [자체점검체크리스트]

2014년 금융권 유출사고 후 금감원은 CEO가 친필사인한 [자체점검체크리스트] 요청

(금융회사내) 고객정보보호 관련 주요현황/체계 및 향후 추진계획

- □ 금 융 회 사 명 :
- □ **대 표 자(CEO)** : (직위) (인)
- □ 정보보호최고책임자(CISO) : (직위) (인)
- □ 개인정보 보호책임자(CPO) : (직위) (인)
- □ 신용정보관리 보호인 : (직위) (인)
- □ 감 사 : (직위) (인)

(금융회사내) 고객정보관리실태 자체점검 체크리스트

- □ 금 융 회 사 명 :
- □ **대 표 자(CEO)** : (직위) (인)
- □ 정보보호최고책임자(CISO) : (직위) (인)
- □ 개인정보 보호책임자(CPO) : (직위) (인)
- □ 신용정보관리 보호인 : (직위) (인)
- □ 감 사 : (직위) (인)

금융회사 **CEO**, CISO, CPO, 신용정보관리인, 감사가 모두 각각 친필사인!

(3) 2013.11.23 시행 전자금융거래법 개정안

〈IT부문계획서〉에 보안실적계획 필수, CEO 확인서명 필수, 매년 금융위원회 제출

법 — 전자금융거래법 제21조 4항 (IT부문계획수립/제출)

신설
매년 IT부문계획을 수립하여 **CEO**의 확인 · 서명을 받아 금융위원회에 제출해야 한다

보안은 **CEO가 책임**져야 하는 사항

구체화 — 전자금융거래법 시행령 제11조의2 (IT부문계획서제출)

신설
③ [IT부문계획서] 포함사항
목표 · 전략 · 조직 · 실적 · 예산 · 추진계획 · 전자금융기반시설의 취약점분석평가내용 및 절차, 취약점분석결과에 따른 보완조치 이행계획, 다음 업무에 대한 실적 및 계획

신설
② [IT부문계획서]는 **매년 3월말**까지 제출

시행령

전자금융거래법 제21조의 2
③ CISO는 다음 각 호의 업무를 수행한다
1. 전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 및 계획의 수립
2. 정보기술부문의 보호 및 관리
3. 정보기술부문의 보안에 필요한 인력관리 및 예산편성
4. 전자금융거래의 사고 예방 및 조치

(뒷장에서 계속)

2. 개인정보보호 책임자로 금융기관 CEO 명시 (앞장에서 계속)

(4) 2013.11.23 발표 금융전산 보안강화 종합대책

취약점 점검 및 보완, 임직원 보안준수여부 정기점검, 보안조직 사기진작을 CEO책임으로 명시

금융전산 내부통제 강화

핵심사항	현재 문제점을	향후 이렇게 개선
CEO 책임하에 취약점 점검 및 보완	동일취약점을 이용한 해킹발생	· **IT자산식별** → 취약점점검 후 조치계획 수립 · 이행여부를 **CEO에 보고**
보안조직의 내부제재권한 강화	보안조직의 권한 부족	· 정보보안조직은 임직원의 보안준수여부를 정기점검, **결과를 CEO 및 CISO에 보고** · **처벌근거를 금융회사 내규에 마련 · 시행**

전산보안인력 사기진작

핵심사항	현재 문제점을	향후 이렇게 개선
CEO 책임하에 사기진작방안 마련	인사 · 성과평가 불리 보안업무 기피	해외연수, 성과평가 가점, 금융보안 석사과정 학비지원, 정부 훈 · 포상 추천 및 금융위원장 표창 수여

발송일
2014. 06

2014년 6월 30일 실시

전자금융거래법 [금융기관검사 및 제재에 관한 규정 시행세칙] 개정실시

원문보기

[적용대상] 금융기관

[실시일자] 2014년 6월 30일

[세칙요약]

개인신용정보 유출시
정직, 감봉, 견책

정보보호 소홀시	
금융기관	임직원
업무정지, 기관경고, 기관주의	정직, 감봉, 견책

변화 01 개인신용정보 단 1건 유출시 견책!

인사고과에 기록, 승진/인사이동 시 불이익

유출	부당이용	제재
50건 이상	500건 이상	정직이상
5건 이상	50건 이상	감봉
1건 이상	5건 이상	견책
-	1건 이상	주의

유출건수
= 정보주체수 × 유출횟수

1명 정보를 다섯 번 유출할 경우
유출건수는 5건(=감봉)

변화 02 정보보호 소홀정도가 높을 경우 기관/직원 업무정지

원인 / 결과	정보보호 소홀정도가 높을 경우		정보보호 소홀정도가 낮을 경우	
	금융기관	임직원	금융기관	임직원
중대	업무정지	정직이상	업무정지	감봉
보통	기관경고	감봉	기관경고	견책
경미	기관주의	견책	-	-

'정보보호소홀'이란 무엇을 의미하는가?

금감원
[기술적 물리적 관리적 보안대책] 미준수를 의미함

금감원 [기술적 · 물리적 · 관리적 보안대책]

원문보기

기술적 물리적 보안대책

근거조항) 신용정보법 시행령 제16조 1항

조	내용	기술적 보호조치
1조 접근통제	① 〈개인신용정보처리시스템〉 접근권한은 필요최소인원에게 부여 ② 취급자 변경시 지체없이 〈개인신용정보처리시스템〉 접근권한변경, 말소 ③ 권한부여, 변경, 말소내역 기록, 최소 3년보관	[DB 접근권한 관리/기록] DB-i
	④ 〈개인신용정보처리시스템〉에 침입차단/침입탐지시스템 설치	[이상징후탐지] DB-i , was-i , App-i
	⑤ 패스워드 작성규칙 수립	
	⑥ 〈개인신용정보〉가 홈페이지, P2P, 공유설정 등으로 공개되지 않도록 〈개인신용정보처리시스템〉 및 취급자 PC 설정	[네트워크DLP] Mail-I™ [서버내 개인정보검출] Server-i
2조 접속기록 위변조방지	① 〈개인신용정보〉 접속기록 저장, 월 1회 이상 확인 · 감독 ② 〈개인신용정보처리시스템〉 접속기록 위변조방지	[개인정보 조회기록보관 및 위변조방지] DB-i , was-i , App-i
3조 개인신용정보 암호화	① 인증정보(패스워드, 생체정보)는 일방향 암호화저장 ② 〈개인신용정보〉 및 인증정보 송 · 수신시 암호화	
	③ 〈개인신용정보〉 PC저장 시 암호화	[PC내 개인정보암호화] Privacy-i
4조 컴퓨터 바이러스 방지	① 바이러스, 스파이웨어 등 악성프로그램 점검 · 치료를 위해 백신 설치	
	② 백신 월1회이상 갱신 · 점검, 바이러스경보/업데이트시 즉시 갱신 · 점검	
5조 출력복사시 보호조치	① 〈개인신용정보〉출력(인쇄, 화면표시, 파일생성 등) 시 용도명확화, 출력항목 최소화 ② 〈개인신용정보〉 매체저장, 이메일 등 외부전송시 사전승인 ③ ①②항준수에 필요한 내부시스템 구축	[파일생성방지] DB-i [엔드포인트DLP] Privacy-i [네트워크DLP] Mail-I™

(뒷장에서 계속)

금감원 [기술적 · 물리적 · 관리적 보안대책] (앞장에서 계속)

관리적 보안대책

조	내용	기술적 보호조치
1조 신용정보관리, 보호인	① 〈신용정보관리, 보호인〉 업무 1. 내부관리규정 제,개정 2. 고충처리 3. 임,직원 신용정보관리, 보호 4. 정보주체권리행사에 대한 이행여부점검 5. 임,직원 교육실시	
	② 〈신용정보관리, 보호인〉은 업무처리기록 3년보존, 점검결과 경영진 보고 및 업무처리절차에 반영	[개인정보 조회기록보관 및 위변조방지] DB-i
2조 개인신용정보 조회권한 구분	① 〈신용정보관리, 보호인〉은 〈개인신용정보〉조회권한을 직급, 업무별로 차등부여	[조회권한관리] DB-i
	② 신용정보회사등은 〈개인신용정보〉조회기록을 주기적점검, 점검결과 업무 반영	[접근기록관리] DB-i
	③ 〈신용정보관리, 보호인〉은 신용조회기록 정확성을 점검	
3조 제재기준	① 신용정보회사는 〈개인신용정보〉오, 남용자체제재기준 마련	

발송일
2014. 05

2014년 5월 28일

[금융지주회사법] 개정시행 원문보기

금융계열사간 개인정보는

조건부 허용 내부경영관리 목적에 한하여 고객정보 제공허용

조건1 신설
[고객정보 제공절차]를
준수해야 함

조건2 신설
[고객정보 제공내역]을
고객에게 통지해야 함

금지

영업, 마케팅목적
제공금지

위반시 과태료 5000만원

고객정보는 내부경영관리목적으로만 제공

개정 제48조의2 (고객정보의 제공/관리)

① 금융지주회사(계열사)는 **금융거래정보/개인신용정보**를 고객정보제공절차에 따라 **내부 경영관리상의 목적**으로 이용될 수 있다.

② 금융지주회사는 위탁자의 **증권총액정보**를 고객정보제공절차에 따라 **내부 경영관리상의 목적**으로 이용될 수 있다.
(증권총액정보: 예탁한 금전/증권의 총액, 예탁한 증권의 종류별 총액, 그밖의 금융위원회가 정한 정보들)

조건1 [고객정보 제공절차] 포함사항

- 제공범위
- 고객정보 암호화 처리방법
- 고객정보 분리보관방법
- 고객정보 이용기간/목적
- 이용기간 경과시 삭제방법
- 대통령령으로 정한 사항 대통령령 제27조의2 2항
  - 고객정보 요청/제공시 고객정보관리인 승인
  - 고객정보 제공/이용관련 점검사항

내부경영관리목적으로 제공

O 신용위험관리, 내부통제, 업무/재산상태검사, 고객분석, 상품/서비스개발, 성과관리, 위탁업무 수행

X 외부영업, 마케팅 등의 업무

조건2 고객에게 고객정보 제공내역 통지

개정 제48조의2 **(고객정보의 제공/관리)**

④ 고객정보를 금융지주회사(계열사) 등에게 제공하는 경우에는 **고객정보제공내역**을 **고객에게 통지**해야 한다.
단, **연락처 등 통지할 수 있는 개인정보를 수집하지 않은 경우에는 통지하지 않는다.**

⑤ **통지해야 하는 정보의 종류, 통지 주기 및 방법, 그 밖의 사항**은 대통령령으로 정한다.
- 정보의 종류 : 고객정보를 제공하는 자/제공받는 자, 고객정보의 제공목적/제공항목,
- 통지 주기 : 연 1회 이상
- 통지 방법 : 우편, 전자우편 등

통지해야하는 [고객정보 제공내역] (대통령령 제27조의2 3항)

고객정보를 제공하는 자	고객정보를 제공받는 자	고객정보의 제공목적	고객정보의 제공항목

규정위반시 **과태료** 부과

개정 **제72조 1항 6호 (과태료)**

48조의2 ①,②,④항의 규정을 위반하는 자는 **5,000만원 이하의 과태료**에 처한다

금융지주회사란?

주식 보유를 통해 은행, 증권, 보험사 등 금융기관을 지배하는 지주(持株)회사

발송일
2014. 04

2014.03.10
6개 중앙부처 (금융위, 금감원, 행자부, 방통위, 미래부, 기재부) 연합으로

금융분야 개인정보유출 재발방지 종합대책 발표

원문보기

신 용정보보호법 전 자금융거래법

2014년 금융권 유출사고 이후 개인정보보호 변화

① 유의사항공표
2014.01.13
'고객정보유출방지를 위한 금융회사 유의사항' 공표

② 전면점검
2014.01~02
전 금융회사 고객정보보호 전면점검

③ 재발방지대책발표
2014.01.22
금융회사고객정보유출 재발방지대책 발표
신 전 개정예정

+

④ 불법유출차단조치 발표
2014.01.24
개인정보 불법유통 차단조치 발표
불법정보 유통 / 활용 집중단속
「불법유통 개인정보 신고센터」 설치

발전/구체화

⑤ 금융분야 개인정보유출 재발방지 종합대책발표

금융위원회 · 금융감독원 FINANCIAL SUPERVISORY SERVICE · 행정자치부 · 방송통신위원회 KOREA COMMUNICATIONS COMMISSION
미래창조과학부 · 기획재정부 MINISTRY OF STRATEGY AND FINANCE
범정부연합 구성/발족

신용정보보호법 전자금융거래법 여신전문금융업법 금융지주회사법 보험업법 개인정보보호법 전기통신사업법 개정 예정 → 금융/공공/민간 전분야 확대예정

금융분야 개인정보유출 재발방지 종합대책 요약

요약1 개인정보 최소보관 유출피해최소화	요약2 금융회사, CEO, 임원 책임확대	요약3 유출정보활용 대출영업 강력제재	요약4 제 3자제공, 내부관리시 소비자피해방지
요약5 과징금/처벌강화	요약6 전산보안대책강화	요약7 정보보안관련 점검/관리강화	요약8 개인정보 보유현황파악 / 대응매뉴얼구축

금융분야 개인정보유출재발방지 종합대책

1) 개인정보 최소보관, 유출시 피해 최소화

핵심사항	현황/문제점	개선방안	기술적 보호조치
개인정보 최소수집	개인정보 과도수집/보유 (20-50종 개인정보 수집)	· 필수/선택항목으로 구분 및 수집최소화 · 필수정보: 이름, 주민번호, 주소, 연락처, 직업, 국적 · 선택정보: 목적, 제공처, 혜택설명, 고객동의 후 수집 · 계약필수사항이 아님을 고지 (비동의불이익 없음) ▶ 개정되는 관련법 **신용정보보호법**	Privacy-i PC내 실태점검 Server-i 서버내 실태점검
주민번호는 최초 거래시에만 수집가능	신용조회, 세금문제로 금융회사는 주민번호를 수집할 수 밖에 없음	· **첫 거래에서만** 전자단말기, 콜센터인증으로 주민번호수집 가능 이후 신분증확인, 인증시스템으로 신원확인	
내부망 저장 주민번호 암호화	외부망 저장시 주민번호암호화	· 내외부망 모두 주민번호 암호화 ▶ 개정되는 관련법 **개인정보보호법**	
거래종료 단계별 고객정보 보관	탈퇴회원 등 거래종료고객정보 계속 보유	1단계: 원칙적으로 필요한 정보만 보관 (이름, 주민번호, 거래정보) 나머지정보는 **3개월이내 파기** (학력, 직업, 직위) 2단계: 금융분쟁에 대비, 1단계서 보관정보는 거래종료 후 **5년이내 모두 파기** (상거래소멸시효 5년)	Privacy-i PC내 개인정보파일 유효기간 설정, 파기
분사 후 개인정보관리	분사 후에도 기존고객정보 보관	· **자사고객이 아닐 경우 이관받지 않음** · 분사이전정보와 연계되어있을 경우엔 별도분리 후 5년이내파기 ▶ 개정되는 관련법 금융지주회사법	Privacy-i ① 삭제 ② 암호화 ③ 네트워크, 출력, USB저장내역기록 Server-i 서버내 정보삭제

금융분야 개인정보유출재발방지 종합대책

2) 금융회사, CEO, 임원책임확대

핵심사항	현황/문제점	개선방안	기술적 보호조치
CISO 책임강화	(보안과 상충하는) 타 IT직위와 겸직가능	타 IT직위와 겸직불가 ▶ 개정되는 관련법 **전자금융거래법**	Privacy consulting
신용정보 관리·보호인을 임원으로 임명	· CEO관심부족 · 임원대상 개인정보보호 보고부족 · 법규준수를 위한 관리체계구축 미흡	· CEO 관리책임 명확화 신용정보보호책임자 ▶ 권한/책임강화 · 신용정보관리/보호인을 임원으로 임명 · 신용정보관리/보호인은 CEO보고 월1회 이상, 이사회보고 연 1회 이상 ▶ 개정되는 관련법 **신용정보보호법**	Privacy consulting

3) 유출정보활용 대출영업 강력제재

핵심사항	현황/문제점	개선방안	기술적 보호조치
대출모집인 자격박탈	대출모집인, 대부중개업자, 보험설계사, 카드모집인 등이 개인정보를 불법유출·이용해도 제재없음 (자격박탈시 2년간 재등록 제한)	· 고객정보 불법유출/사용시 대출모집인, 보험설계사 등 자격박탈 → **5년간 재등록 제한** (사실상 영구퇴출)	[네트워크 DLP] Mail-i [엔드포인트 DLP] Privacy-i
금융회사의 대출모집인 관리책임	금융회사의 관리적 책임규정 미흡	· 대출모집인의 잘못은 금융회사 직원의 잘못 **금융회사 제재, 과징금부과** · 대부중개업자가 법인(회사)일 경우 임직원 제재 / 과징금부과 ▶ 개정되는 관련법 **신용정보보호법, 대부업법**	[대출모집인 개인정보 보유활용 실태점검] · PC내 실태점검 Privacy-i · 서버내 실태점검 Server-i [금융회사에서 대출모집인으로의 개인정보전송통제] · 네트워크전송통제 Mail-i · 출력, 저장매체 전송통제 Privacy-i
유출정보를 활용한 범죄피해 예방	대출사기, 보이스피싱 등 정보통신망을 통한 범죄수단 차단기술 미흡	· **정보통신망 이용범죄 사전차단** · 불법대부광고, 금융사기 전화번호차단 · 발신조작번호차단 or 정상번호전환 · 스미싱(문자메시지사기) 의심문자 발송차단 · 미등록 계좌번호에는 소액이체만 가능 (1일 최대100만원)	

금융분야 개인정보유출재발방지 종합대책

4) 제 3자제공 or 내부관리시 소비자피해방지

핵심사항	현황/문제점	개선방안	기술적 보호조치
제3자제공시 필수·선택사항 구분	필수 · 선택사항 구분없이 포괄적으로 정보제공	· 제 3자 제공시 필수/선택사항분리 · 선택사항의 경우 정보주체는 정보를 제공하고 싶은 제 3자만 선택해서 정보를 제공할 수 있음 ▶ 개정되는 관련법 **신용정보업감독규정**	Privacy consulting
제3자제공시 활용기간명시	'정보활용목적이 다 한 경우' 등으로 포괄적 규정	· 제3자제공 정보의 내용/목적/업체명/기간/파기계획 구체적 명시 · 이용기간이 끝난 경우 파기 · 제3자는 **금융회사에 파기확인서 제출** ▶ 개정되는 관련법 **신용정보보호법**	Privacy-i PC내 실태점검, 파기 Server-i 서버내 실태점검
금융그룹 내 활용제한	**금융지주회사법상 특례**에 따라 고객동의없이 정보제공가능	· (내부경영관리를 위한) **신용위험관리, 고객분석은 허용** · (동의없이)고객정보를 **외부영업에 활용시 절차강화** 현행: 고객정보관리인 승인 개선: 이사회승인 / 이용내역 고객통지 ▶ 개정되는 관련법 금융지주회사법, 금융지주회사의 고객정보업무지침서	[네트워크 DLP] Mail-i [엔드포인트 DLP] Privacy-i

금융분야 개인정보유출재발방지 종합대책

5) 과징금 및 처벌강화

<table>
<tr><th>핵심사항</th><th>현황/문제점</th><th>개선방안</th><th>기술적보호조치</th></tr>
<tr><td>과징금
대폭상향</td><td>금융회사 (전속 대출모집인포함) 가
정보유출 ·
유출정보 활용시
금전적 제재 미흡</td><td>① 금융회사(전속 대출모집인포함)가
불법수집/유통된 개인정보를 활용하여 영업시
· 과징금
· 형벌(3년이하 징역, 3천만원 이하 벌금)
· 과태료(1천만원 이하)
▶ 개정되는 관련법 신용정보보호법

② 개인정보유출/활용한 금융회사(전속 대출모집인포함에
과징금부과
<table><tr><th>개인정보 유출 유형</th><th>과징금</th></tr><tr><td>불법적 개인정보유출</td><td>관련매출액 3%이하(관련매출 10조 경우 3천억원)</td></tr><tr><td>관리소홀로 인한 유출</td><td>최대 50억원 과징금부과</td></tr></table>
③ 주민번호 불법활용/유출시
다른 일반 개인정보(주소, 나이, 연락처 등) 유출시보다
과태료 · 과징금 가중하여 부과

④ '정보유출방지 주의의무' 위반시 과태료수준 대폭강화
▶ 개정되는 관련법 신용정보보호법, 전자금융거래법
<table><tr><th colspan="2">정보유출방지 주의의무 해당 규정</th><th>과태료</th></tr><tr><td rowspan="3">신용
정보
보호법</td><td>정보유출방지보안장치 미비</td><td>기존 6백만원→
5천만원으로 강화</td></tr><tr><td>정보보호관리인이 CEO에
정보보호관련 보고의무 태만</td><td>5천만원(신설)</td></tr><tr><td>식별정보
암호화조치/폐기의무 위반</td><td>3천만원(신설)</td></tr><tr><td>전자금융
거래법</td><td>안전성확보의무위반
(전자금융거래법 21조)</td><td>5천만원(신설)</td></tr></table></td><td>[네트워크 DLP]
Mail-i

[엔드포인트 DLP]
Privacy-i
PC내 실태점검

Server-i
서버내 실태점검</td></tr>
</table>

<table>
<tr><th>핵심사항</th><th>현황/문제점</th><th>개선방안</th><th>기술적 보호조치</th></tr>
<tr><td>처벌수준
강화</td><td>현재 형량이 낮음
[개인정보유출 관련법령상 형량수준]
<table><tr><th>법</th><th>신용정보보호법</th><th>전자금융거래법</th><th>개인정보보호법</th></tr><tr><td>법적용
대상</td><td>신용정보
제공/이용자
(은행, 카드 등)</td><td>전자금융업자
(금융회사 등)</td><td>모든
개인정보처리자</td></tr><tr><td>유출자
형량</td><td>5년이하 징역 or
5천만원이하 벌금</td><td>7년이하 징역 or
5천만원이하 벌금</td><td>5년이하 징역 or
5천만원이하 벌금</td></tr></table></td><td>금융관련법 최고수준인
10년이하 징역
5억원이하 벌금
(은행법 제66조) 으로 상향</td><td>[네트워크 DLP]
Mail-i
[엔드포인트 DLP]
Privacy-i</td></tr>
</table>

금융분야 개인정보유출재발방지 종합대책

6) 전산보안대책강화

핵심사항	현황/문제점	개선방안	기술적 보호조치
주민번호 암호화	영향평가, 위험도분석에 따라 암호화	· 내부망 고객정보DB에 저장된 주민번호는 영향평가, 위험도분석 결과에 상관없이 암호화 ▶ 개정되는 관련법 개인정보보호법	Privacy consulting
망분리	전산센터는 의무화 본점 · 영업점은 단계적/선택적 추진	· 전산센터는 2014년말, 은행본점/영업점은 2015년말 완료 · 금감원 정기점검. 미이행시 기관 및 책임자 제재	
금융전산 모니터링 서비스	[적용업종] 은행, 증권 [설치범위] 금융거래시스템	· [적용업종확대] (은행 증권 외에) 보험, 카드사까지 적용 · [설치범위 확대] (금융거래시스템 외에) 홈페이지까지 적용 ▶ 개정되는 관련법 **전자금융거래법개정**	
금융전산 보안인증제	금융분야에 특화된 보안관련 인증제 없음	· 보안관리수준을 평가하는 [금융전산 보안인증제] 도입 ▶ 개정되는 관련법 **전자금융법규개정**	Privacy consulting

금융분야 개인정보유출재발방지 종합대책

7) 정보보안관련 점검관리강화

핵심사항	현황 / 문제점	개선방안	기술적 보호조치
CISO 책임하에 외주업체 관리강화	〈외주용역통제규정〉은 있으나 편의를 추구하다가 사고발생	[CISO책임] · 외부저장매체(노트북, USB등) 반입통제 · 금감원검사시 〈외주용역통제규정〉 준수여부를 우선 점검 · 핵심사항은 〈외주용역일일체크리스트〉로 관리 외주용역 일일체크리스트 외주용역 정보유출사고 예방위한 보안통제 점검항목으로 구성 1. 업무통제: 고객정보 사용내역관리 2. PC관리: 보안프로그램설치, PC내 고객정보 보관금지 3. 전산기기 반출입 및 외부인력통제: USB봉인, 외부인 출입관리 등	Privacy-i PC내 실태점검 Server-i 서버내 실태점검
〈금감원〉 철저점검	내부통제규정이 실행단계에서 제대로 지켜지지 않음	〈금융회사〉 · 자체 보안규정보완/구체화 · 규정준수여부를 CISO 책임하에 매월 점검(보안점검의 날 지정) · 취약점 즉시 보완→CEO에게 결과보고 · 업무별/직급별 고객정보 접근권한 범위를 명확히 하는 [보안등급제]추진 〈금감원〉 · 법규준수여부 철저점검, 엄중 제재 · 불시점검 **기동점검반** 운영	[DB방화벽] DB-i 접근권한통제 Privacy-i PC내 실태점검 Server-i 서버내 실태점검

8) 개인정보 보유현황파악 및 대응매뉴얼구축

핵심사항	현황 / 문제점	개선방안	기술적 보호조치
금융회사 개인정보 보유현황점검 /파기	거래종료고객정보 계속 보유	전면점검실시(2014.02~) · 계약유지, 법률의무이행에 필요한 정보만 보관 · 점검이후 불필요정보 불법활용 및 유출시 엄중제재	Privacy-i PC내 실태점검 Server-i 서버내 실태점검
대응매뉴얼 구축	사내 대응매뉴얼 미흡	개인정보유출사고 대비 CEO 책임 하 대응매뉴얼 구축	Privacy consulting

발송일
2014. 02

금감원, 금융권 3,050개사 대상 [자체점검 체크리스트] 배포

은행, 보험, 증권, 카드, 캐피탈, 저축은행, 상호금융 등 3,050개 금융기관

2014년 2월 14일까지 금융감독원 제출

금융감독원 2014년 3월중 현장점검 착수

금융감독원 2014년 1월 13일 금융회사 정보보호 임원회의 개최 [고객정보보호대책] 발표

① 공표완료
[고객정보 유출방지를 위한 금융회사 유의사항] 공표

② 점검
전 금융회사 고객정보보호 전면점검

③TF설립
2014.1.22,
[금융회사 고객정보 유출재발방지대책] 발표
▶ 신용정보보호법, 전자금융거래법 개정 예정

④ 〈정보유출감시센터〉 금감원에 설치
▶ (행자부 118처럼)
금융기관 개인정보오남용 신고전화1332 개설

금융권 3,050개사 대상
[자체점검 체크리스트] 배포, 이후 현장점검

제출문서 1

(금융회사내) 고객정보보호 관련 주요현황/체계/향후 추진계획

□ 금 융 회 사 명 :
□ 대 표 자 : (직위) (인)
□ 정보보호최고책임자(CISO) : (직위) (인)
□ 개인정보 보호책임자(CPO) : (직위) (인)
□ 신용정보관리 보호인 : (직위) (인)
□ 감 사 : (직위) (인)

제출문서 2

(금융회사내) 고객정보관리실태 자체점검 체크리스트

□ 금 융 회 사 명 :
□ 대 표 자 : (직위) (인)
□ 정보보호최고책임자(CISO) : (직위) (인)
□ 개인정보 보호책임자(CPO) : (직위) (인)
□ 신용정보관리 보호인 : (직위) (인)
□ 감 사 : (직위) (인)

금융회사 대표, CISO, CPO, 신용정보관리인, 감사가 모두 각각 친필사인!

제출문서 1 (금융회사내) 고객정보보호 관련 주요현황/체계/향후 추진계획

1) 고객정보보호 주요현황

점검항목	기입정보	기술적 보호조치
1. 보유 〈**고객정보**〉	업무구분, **정보명**, **고객수**	Privacy-i PC내 실태점검 Server-i 서버내 실태점검
2. **보유고객구분**	현재거래고객수, 거래종료고객수, 제휴고객수	
3. 수집하고 있는 〈**고객정보**〉종류 및 개수	업무구분, 서식명, 정보명, 정보수, **제외가능한 정보명 및 개수**	
4. 〈**고객정보**〉처리가 수반되는 외부위탁/용역/제휴현황	상대회사명, 계약기간, 업무, **상대회사가 접근 가능한 고객정보**, 점검여부, 점검결과	
5. 〈**고객정보**〉 다운로드에 대한 사후점검	점검주관, 기간, 방법, 결과, 조치사항	
6. 〈**고객정보**〉 부당유출	**유출일시**, **유출자**, **원인**, **유출정보건수**, **유출상대**, 조치내용	[Network DLP] Mail-i [EndPoint DLP] Privacy-i
7. 〈**고객정보**〉 부당유출 점검	점검주관, 점검기간, 점검방법, 점검결과	
8. 텔레마케팅〈**고객정보**〉	업체명, 업무, 제공정보(내역 및 개수), **계약종료 후 고객정보처리방법**, TM직원수	Privacy-i 파기
9. 〈CPO〉 및 〈**신용정보관리보호인**〉 지정	· 〈CPO〉 직급, 임명일, 겸임시직위, 개인정보보호조직, 인력 · 〈**신용정보관리보호인**〉직급, 임명일, 겸임시직위 신용정보관리보호조직, 인력	
10. IT(보안) 인력, 예산, 조직	IT(보안) 인력, 예산, 조직	
11. 〈CISO〉 및 **[보안내규] 지정**	연간 [전사적 IT보안계획]최종보고대상 · 〈CISO〉 직급, 자격 충족여부, 임명일, 겸임업무직위 · **[IT보안 내규]** 지침 수, 외부주문에 대한 내부통제 조직, 인력	
12. [정보보호시스템] 운영	**DB암호화**, **DB접근통제**, DLP, **PC정보보호관리솔루션** 보유여부	DB-i DB접근통제 Privacy-i PC정보보호 [Network DLP] Mail-i [EndPoint DLP] Privacy-i

제출문서 1 (금융회사내) 고객정보보호 관련 주요현황/체계/향후 추진계획

2) 고객정보 보호체계현황

점검항목	기입정보	기술적 보호조치
1. 조직(인력 포함) 및 주요업무	조직, 인력현황, 주요업무	
2. 내부통제제도 및 관리체계	내규, 지침, **접근권한통제현황**	DB-i DB접근통제
3. 외주업체(외주직원) 관리체계	· 관리조직현황(일반업무, IT업무 구분) · 주요 외주업체 통제실시현황	
4. 전산자료 보호대책	· 사용자계정/비밀번호 관리 및 **전산자료 접근권한 통제** · 전산자료/전산기기 반출입, **보조기억장치 통제** · 테스트시 자료변환, **단말기 이용자정보보관** · **전산자료 · 정보처리시스템 접근기록 관리**	DB-i ①DB접근통제 ②접근기록관리 Privacy-i ① 보조기억 장치통제 ② 단말기 이용자 정보 보관 통제
5. 자체감사 및 점검체계	· 내부감사/통제 조직 및 인력 · 2013년 실적, 2014년 계획	

3) 향후 고객정보 보호관련 업무추진 계획

점검항목	주요사항
1. 단기계획(2014년)	ex) 내부통제관리체계강화, 정보유출방지시스템 도입실시 및 계획이 있다
2. 중장기계획(2015~2016년)	

4) 고객정보 보호체계관련 우수사례

점검항목	주요사항
1. 내부통제 부문	추진배경, 추진 전 문제점, 추진내용, 기대효과
2. IT부문	

제출문서 2 금융회사, 고객정보관리실태 자체점검 결과표

개 : 개인정보보호법
신 : 신용정보보호법
전 : 전자금융거래법

개 고시 : 개인정보보호법 고시 [개인정보의 안전성 확보조치 기준]
신 고시 : 신용정보보호법 고시 [신용정보업감독규정]
전 고시 : 전자금융거래법 고시 [전자금융감독규정]

내부통제부문 1) 고객정보 관련규정 및 절차 수립

개	신	전	점검항목
	· 법 20조 · 고시 22조		① [내부관리규정]
· 법 29조 · 시행령 30조 · 고시 3조			② [내부 관리계획] ex) 〈개인정보보호책임자〉 지정, [안전성 확보조치], 임직원 교육 등
	· 법 19조 · 고시 별표3		③ 〈고객정보〉 오남용에 대한 [자체제재기준]

내부통제부문 2) 고객정보 수집 및 제3자 제공

미흡한 항목이 있다면?

개	신	전	점검항목	점검결과		기술적 보호조치
				양호	미흡	
법 16조			① 최소수집			
· 법 21조 · 시행령 16조			② 기간경과, 목적달성 등 불필요하게된 경우 지체없이 **복구/재생되지 않도록 파기**		✓	Privacy-i 파기기능
법 17조, 22조			③ 수집/이용/제공 동의시 〈일괄동의〉, 〈포괄적동의〉 금지			

제출문서 2 금융회사, 고객정보관리실태 자체점검 결과표

내부통제부문 3) 고객정보 이용통제

개	신	전	점검항목	점검결과 양호	점검결과 미흡	기술적 보호조치
고시 4조	고시 별표3	고시 13조	① 계정부여시 **권한최소화** (직급별, 업무별, 내외부직원별로 구분), **통제장치보유**		✓	DB-i, was-i ① 접근권한통제 ② 접근기록관리 ③ 권한초과, 일정횟수 이상 조회시도 직원통제, 조회건수 급증한 직원 점검
			② 〈**고객정보**〉조회(활용)시 조회자 신원, 조회일시, 대상정보, 목적, 용도 등 기록관리		✓	
			③ 〈**고객정보**〉 **과다조회부서/직원 수시점검** · **권한초과, 일정횟수 이상 조회시도한 직원에 대한 통제장치** · **조회건수 급증한 직원 점검**		✓	

내부통제부문 4) 고객정보 관리책임자 역할

개	신	전	점검항목	점검결과 양호	점검결과 미흡	기술적 보호조치
법 31조	· 법 20조 · 시행령 17조		① 책임자(CPO, 신용정보관리보호인 등)가 임직원 법규준수여부를 점검하는가?			
			② 임직원 대상 〈개인정보보호교육〉을 실시하는가?			
		고시 13조	③ 단말기에 개인정보 보관/공유 금지 * 부득이한 경우 책임자 승인하에 시행		✓	Privacy-i PC내 개인정보 검출, 파기 암호화 ,결재

제출문서 2 금융회사, 고객정보관리실태 자체점검 결과표

내부통제부문 5) 고객정보유출시 사고대응체계

개	신	전	점검항목	점검결과 양호	점검결과 미흡	기술적 보호조치
법 34조		고시 73조	① 유출시 [감독당국신고], [고객유의사항안내] 등 [사고대응체계] 규정화, 이행			
			② 유출시 지체없이 유출된 〈고객정보〉항목, 시점, 경위, 피해구제절차 등을 정보주체에게 통지		✓	[Network DLP] Mail-i [EndPoint DLP] Privacy-i

내부통제부문 6) 고객정보 외주업체 통제 (IT외주업체 제외)

개	신	전	점검항목	점검결과 양호	점검결과 미흡	기술적 보호조치
법 26조	법 17조	고시 60조	① 위탁계약서의 적정성여부 * 제공되는 〈고객정보〉범위, 제공/이용목적, 업무목적외 사용/제3자 제공금지, 정보유출방지, 폐기/반납에 관한 사항 등			
			② 〈고객정보〉가 분실/도난/유출/변조/훼손되지 않도록 외주업체교육 및 점검		✓	Privacy-i PC내 실태점검 Server-i 서버내 실태점검
			③ 외주업체가 사전동의 없이 다시 외부주문 등 계약을 체결하거나 계약업체를 변경하지 못하도록 통제			

제출문서 2 금융회사, 고객정보관리실태 자체점검 결과표

IT 부문 정보보호 대책 1) 계정 / 비밀번호 관리

개	신	전	점검항목	점검결과		기술적 보호조치
				양호	미흡	
		고시 13조	① 직원(외부직원포함) 인사변경, 계약만료시 지체없이 계정삭제/중지, 공동계정변경 등 [정보처리시스템]접근통제		✓	DB-i DB접근통제
	고시 별표3	고시 32조, 33조	② 〈내부사용자〉, 〈이용자〉 비밀번호작성규칙 수립/적용			

IT 부문 정보보호 대책 2) 고객정보 암호화 / 변환 사용

개	신	전	점검항목	점검결과		기술적 보호조치
				양호	미흡	
고시 7조	고시 별표3		① 〈비밀번호〉, 〈바이오정보〉 일방향암호화			
법 24조		고시 17조	② 공개용망(DMZ등)에 〈고유식별정보〉 보관시 암호화 (내부망은 위험도분석결과에 따라 적용) ※ 암호화대상 : 고유식별정보(주민번호, 여권번호, 운전면허발급번호, 외국인 등록번호)		✓	Privacy-i ①PC내 암호화 ②파기 DB-i, was-i 송수신시암호화 Server-i 서버내 암호화
고시 7조	고시 별표3		③ 정보통신망을 통해 〈고객정보〉송수신, PC저장시 암호화		✓	
		고시 13조	④ [정보처리시스템]개발, 테스트시 〈고객정보〉 변환사용, 테스트종료 즉시 삭제		✓	

IT 부문 정보보호 대책 3) 정보처리시스템보안

개	신	전	점검항목	점검결과		기술적 보호조치
				양호	미흡	
고시 6조	고시 별표3	고시 15조	① 해킹사고방지를 위한 [정보보호시스템] 설치/운영 * 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 침입차단/침입탐지 등 설치 · 운영		✓	DB-i, was-i ①침입차단/탐지 ②접속기록위변조방지 ③전송시 DB VPN적용
고시 8조		고시 3조	② [고객정보저장시스템]접속기록 위/변조방지보관, 도난, 분실방지		✓	
고시 6조		고시 15조	③ 외부망을 통한 시스템접속시 VPN or 전용선 등 적용		✓	

제출문서 2 금융회사, 고객정보관리실태 자체점검 결과표

IT 부문 정보보호 대책 4) 정보에 대한 접근통제

개	신	전	점검항목	점검결과		기술적 보호조치
				양호	미흡	
		고시 12조	① 모든단말기에서 사용자의 주요업무 **로그기록, 접근제어,** 무선통신망관리 등 보호대책 수립		✓	[Network DLP] Mail-i [EndPoint DLP] Privacy-i
	고시 별표3		② [**고객정보처리시스템**]에서 출력시 (인쇄, 화면표시, 파일생성 등) **용도특정, 출력항목 최소화**		✓	DB-i, was-i ① 인쇄, 파일생성 차단 ② 용도특정, 출력항목 최소화
		고시 19조의2	③ 임직원 [정보보호교육계획] 수립/시행			

IT 부문 정보보호 대책 5) PC보안

개	신	전	점검항목	점검결과		기술적 보호조치
				양호	미흡	
		고시 12조	① 중요단말기 보안대책강화 (외부반출금지, 업무전용 단말기지정/지정용도외 사용금지, **인터넷 접속금지** 등) 수립		✓	WebKeeper P2P등 유해사이트 / 악성코드배포 사이트 접속차단 Mail-i 네트워크DLP
고시 6조	고시 별표3		② 〈**고객정보**〉가 홈페이지, P2P, 공유설정 등을 통하여 공개되지 않도록 PC통제		✓	
고시 9조		고시 16조	③ 백신 등 보안프로그램 설치/업데이트			
		고시 15조	④ 우회 무선통신망 접속 차단을 위한 시스템 구축/모니터링 실시			
		고시 12, 13조	⑤ 〈보조기억매체〉 보유현황/관리실태 점검, 사용통제			
	고시 별표3	고시 12조	⑥ 〈보조기억매체〉 차단통제프로그램을 모든 단말기에 설치/운영하는가?		✓	Privacy-i 보조기억매체에 개인정보저장 차단, 기록, 결재

제출문서 2 금융회사, 고객정보관리실태 자체점검 결과표

IT 부문 정보보호 대책 6) 전산실 / 자료 통제

개	신	전	점검항목	점검결과		기술적 보호조치
				양호	미흡	
		고시 12조	① 모든단말기에서 사용자의 주요업무 **로그기록, 접근제어**, 무선통신망관리 등 보호대책 수립		✓	[Network DLP] Mail-i [EndPoint DLP] Privacy-i
	고시 별표3		② **〈고객정보처리시스템〉에서 출력시** (인쇄, 화면표시, 파일생성 등) **용도특정, 출력항목 최소화**		✓	DB-i, was-i ① 인쇄, 파일생성 차단 ② 용도특정, 출력항목 최소화
		고시 19조의 2	③ 임직원 [정보보호교육계획] 수립/시행			

IT 부문 정보보호 대책 7) IT 외주업체 통제

개	신	전	점검항목	점검결과		기술적 보호조치
				양호	미흡	
		고시 12조	① 중요단말기 보안대책강화 (외부반출금지, 업무전용 단말기지정/지정용도외 사용금지, **인터넷 접속금지** 등) 수립		✓	WebKeeper P2P등 유해사이트 / 악성코드배포 사이트 접속차단 Mail-i 네트워크DLP
고시 6조	고시 별표3		② **〈고객정보〉**가 홈페이지, P2P, 공유설정 등을 통하여 공개되지 않도록 PC통제		✓	
고시 9조		고시 16조	③ 백신 등 보안프로그램 설치/업데이트			
		고시 15조	④ 우회 무선통신망 접속 차단을 위한 시스템 구축/모니터링 실시			
		고시 12, 13조	⑤ 〈보조기억매체〉 보유현황/ 관리실태 점검, 사용통제			
	고시 별표3	고시 12조	⑥ 〈보조기억매체〉 차단통제프로그램을 모든 단말기에 설치/운영하는가?		✓	Privacy-i 보조기억매체에 개인정보저장차단, 기록, 결재

발송일
2014. 01

금감원 일제점검대비
[고객정보 유출방지를 위한 금융회사 유의사항]
1~2월중 전 금융회사 고객정보보호 전면점검

원문보기

금융감독원 FINANCIAL SUPERVISORY SERVICE 2014년 1월 13일 금융회사 정보보호 임원회의 개최 [고객정보보호대책]발표

① 공표완료	② 1~2월중	③TF설립 후	④ 1월중
[고객정보 유출방지를 위한 금융회사 유의사항] 공표	전 금융회사 고객정보보호 전면점검	고객정보보호 강화방안 마련 ▶ 법규강화	〈정보유출감시센터〉 금감원에 설치 (행자부 118처럼) 금융기관 개인정보 오남용 신고전화1332 개설

고객정보는
개인정보, 신용정보,
금융거래정보를 의미

금융기관은 신속히
[개인정보보호법], [전자금융거래법], [신용정보보호법]
준수여부를 자체점검, 보완해야 함

고객정보유출방지를 위한 금융회사 유의사항

고객정보관리 내부통제 부문

항목	규정	기술적 보호조치
규정 & 절차점검	고객정보 관리, 처리규정, 절차 점검	행자부지정 영향평가기관으로 컨설팅 제공
접근통제 & 권한 관리	· 조회권한을 직급별, 업무별, 내/외부직원별로 차등 부여 · 과다조회 부서, 직원대상 정기/수시 점검	· was-i 웹애플리케이션을 통한 개인정보오남용방지 - 외부 WAS를 통한 접속자의 DB조회권한제한 - 소량조회를 반복하여 대량을 조회해도 적발 - 정기적 접속기록검색으로 과다조회자 추적 · DB-i DB조회권한관리, 과다조회 부서/직원 점검

(뒷장에서 계속)

고객정보유출방지를 위한 금융회사 유의사항

고객정보관리 내부통제 부문 (앞장에서 계속)

항목	규정	기술적 보호조치
접근통제 & 권한 관리	개인정보를 저장 /외부전송하는 수단통제 (ex,USB)	· DLP(네트워크DLP, 엔드포인트DLP) - 네트워크, 이동식매체, 출력물을 통한 전송통제 - USB저장/출력시 부서장결재, CPO보고용 리포트생성 · Server-i 서버(웹서버, DB서버 등)내 무단저장된 개인정보 검출
	· 고객정보 조회 후 PC저장 기록 보관, 정기점검 · 고객정보 조회 후 출력 기록 보관, 정기점검	· DB-i DB블랙박스기능 DB에서 고객정보조회후 PC저장시 블랙박스 처럼 촬영, 동영상기록 보관 · Privacy-i - PC내 저장된 개인정보검출 - 개인정보출력시 결재, 기록, 차단, 경보
이용 & 제3자 제공 모니터링	· 외주업체 등 제3자 고객정보 제공을 통제 · 보유기간 경과, 처리목적 달성 고객정보 파기	· DLP(네트워크DLP, 엔드포인트DLP) · Privacy-i - 고객정보유효기간설정 - 보유기간경과고객정보검색 - 복구재생불가능하도록 완전파기
교육 & 사고대응 체계 운영	· 고객정보보호교육 정기실시 · 고객정보 유출관련 사고보고, 고객안내 등 사고대응체계 마련	· 행자부지정강사교육 (연간100회이상 교육시행중) · 행자부지정영향평가기관으로 컨설팅 제공

고객정보유출방지를 위한 금융회사 유의사항

외주업체 보안관리

항목	규정	기술적 보호조치
외주업체 및 외주인력 관리강화	보안전담조직에서 아웃소싱업체 보안관리 철저히 수행	
아웃소싱 상주직원 시스템 접근통제 강화	**아웃소싱직원의 자료유출경로차단대책 수립** - DB접속권한 제한 - DB작업내역 자동저장 - 외부반출 통제	·was-i 웹애플리케이션을 통한 개인정보최종조회자 추적 - 외부 WAS를 통한 접속자의 DB접속권한제한 - 접속기록저장 - 소량조회를 반복하여 대량을 조회해도 적발 - 접속기록검색을 통하여 과다조회자 추적 ·DB-i - DB접속권한제한, 접속기록저장 - 과다조회 부서/직원 점검 · DLP(네트워크DLP, 엔드포인트DLP) - 사외이동시 PC에서 매체저장차단, 출력차단 - 네트워크, 이동식매체, 출력물을 통한 고객정보외부반출통제
외주업체의 고객정보 이용통제	**외주업체와 업무계약 만료시** - 외주업체 보유 고객정보 파기 - 사전 동의 없이 제3자 제공 금지	·Server-i, Privacy-i - 외주업체 보유 서버, PC내 개인정보 검출 및 완전파기 · DLP(네트워크DLP, 엔드포인트DLP) - 네트워크, 이동식매체, 출력물을 통한 개인정보 전송통제

고객정보유출방지를 위한 금융회사 유의사항

고객정보보호를 위한 정보기술 부문

항목	규정	기술적 보호조치
사용자 비밀번호 관리 강화	· 비밀번호 정기변경(분기 1회) · 보관시 암호화 · 시스템마다 관리자비밀번호를 다르게 부여하는지 점검	· 기술적 보호조치 접속비밀번호는 일방향 암호화되어 저장
시스템개발시 고객정보 보안통제강화	· 시스템개발시 고객정보 변환사용 · 테스트 후 고객정보삭제여부점검	· Server-i, Privacy-i 서버, PC내 고객정보 완전파기
내외부직원의 PC, 인터넷사용 보호조치 강화	· 직원PC에 고객정보/금융거래정보 보관금지 · 업무상 불가피한 경우 [정보유출방지대책] 수립 · 책임자 승인/보관내역 관리 · 방화벽 우회 인터넷접속 차단 등	· DLP(네트워크DLP, 엔드포인트DLP) - 직원PC내 고객정보 검출, 완전파기 - 네트워크전송, 출력, USB저장시 결재/차단/기록 · WebKeeper - 방화벽 우회 인터넷접속차단

발송일
2013. 09

전자금융거래법 구체화

대통령령(=시행령) 2013년 11월 23일부터 시행

원문보기

전자금융거래법 개정안

제9조 1항 (금융회사의 책임)

① 금융회사는 다음 사고로 이용자에게 손해가 발생한 경우, 손해배상책임을 진다

법

기존
접근매체의 위조나 변조로
발생한 사고

기존
계약체결 or 거래지시의
전자적 전송이나
처리과정에서 발생한 사고

신설
현금자동지급기, 자동입출금기, 지급용단말기,
컴퓨터, 전화기, 휴대폰 등 정보전송 / 처리장치

전자금융거래를 위한 전자적 장치 or
(망법에 따른) 정보통신망에 침입하여
거짓이나 그 밖의 부정한 방법으로
획득한 접근매체 이용으로
발생한 사고

현금카드, 신용카드, OTP, 공인인증서, 이용자ID,
비밀번호, 생체정보 등 전자금융거래 및 인증을 위한 정보

2014년 1월부터
해킹사고시
금융회사가
배상책임을 져야 함

구체화

제9조 2항

② 다음 경우 책임의 전부 or 일부를 이용자에게 부담하게 할 수 있다.

1. 이용자의 고의/과실로 사고발생시, 그 책임을 이용자가 진다는 약정을 체결한 경우
2. 금융회사가 보안절차를 수립/철저히 준수하는 등 합리적인 주의의무를 다한 경우

전자금융거래법 시행령 개정안 핵심사항1

[제8조] 이용자의 고의/과실을 구체화

시행령

기존
1. 접근매체를 제3자에게
대여/위임/양도/담보제공한 경우

기존
2. (제3자가 접근매체를 이용,
전자금융거래할 수 있음을 알고도)
접근매체를 누설/노출/방치한 경우

신설
3. 이용자가 금융기관이 보안상 요구한
[본인확인절차]를 거부하여 사고가 발생한 경우

신설
4. [본인확인절차]를 거친 경우에도
이용자가 1호/2호 행위를 하여 사고가 발생한 경우

전자금융거래법 개정안

법

제21조 4항 (IT부문계획 수립/제출)
금융회사는

신설

매년 IT부문계획을 수립하여
CEO의 확인/서명을 받아
금융위원회에 제출해야 한다.

보안은 CEO가 책임져야 하는 사항임

구체화

전자금융거래법 시행령 개정안 핵심사항2

시행령

[제11조의2] IT부문계획서 제출

신설

③ [IT부문계획서] 포함사항
목표/전략/조직/실적/예산/추진계획/
전자금융기반시설의 취약점분석평가내용 및 절차,
취약점분석결과에 따른 보완조치 이행계획
다음 업무에 대한 실적 및 계획

신설

② [IT부문계획서]는 매년 3월말까지 제출

전자금융거래법 제21조의2 3항

③ CISO는 다음 각 호의 업무를 수행한다.

1. 전자금융거래의 안정성 확보, 이용자 보호를 위한 전략, 계획의 수립
2. 정보기술부문의 보호 및 관리
3. 정보기술부문의 보안에 필요한 인력관리 및 예산편성
4. 전자금융거래의 사고 예방 및 조치

전자금융거래법 개정안

제21조 3항 (전자금융기반시설에 대한 취약점 분석 · 평가)

금융회사는

법

신설

① 다음 사항에 대하여 취약점분석 · 평가를 실시하여 금융위에 결과보고
전자금융기반시설의 IT부문조직, 시설, 내부통제, 전자적장치, 접근매체
전자금융거래 유지를 위한 침해사고대응조치

▶ 전자금융기반시설이란?전자금융거래에 이용되는 정보처리시스템 및 정보통신망

위반시 과태료
최대 2천만원

신설

② 금융위가 ①항의 결과에 대한 이행실태점검/보완조치를 실시할 수 있다

구체화

전자금융거래법 시행령 개정안 핵심사항3

[제11조 4~5항] 취약점 분석평가 부분

시행령

신설

제11조의4

1. IT 외부위탁시 조직,시설,내부통제/전자적장치/접근매체/침해사고 대응조치를 취약점 분석평가
2. [전자금융보조업자]의 정보처리시스템도 취약점 분석평가대상임

신설

제11조의5

① 전자금융기반시설 정기적 [취약점 분석평가]
② 다음 경우, 즉시 or 사전에 [취약점분석평가] 실시
1. IT부문 기능개선/변경시
2. 침해사고발생으로 긴급조치 필요시
3. 시스템, 홈페이지 등 IT부문 사업을 실시한 경우
③ 자체전담반 or [평가전문기관]을 통해 실시
④ [평가전문기관]의 내부정보유출방지조치 실시, 평가재위탁금지
⑤ 종료 후 30일 내 [결과보고서] 금융위원회에 제출

전자금융거래법 개정안

제21조 4~5항 (전자적 침해행위 금지 및 침해사고 대응)

금융회사는

법

신설

제21조 4항 (전자적 침해행위의 금지)

▶ 전자적침해행위 (해킹, 바이러스, 논리 · 메일폭탄, 서비스거부, 고출력전자기파 등)으로 전자금융기반시설을 공격하는 행위

→ 위반시 형사처벌 (7년이하 징역 or 5천만원 이하 벌금)

신설

제21조 5항 (침해사고의 통지 등)

① 침해사고 발생시 금융위원회에 지체없이 통지해야 한다

▶ 침해사고 : 전자적 침해행위로 인하여 전자금융기반시설이 교란, 마비되는 사고

→ 위반시 과태료 (2천만원이하)

구체화

전자금융거래법 시행령 개정안 핵심사항4

[제11조 6~7항] 전자적 침해행위 금지 및 침해사고 대응

시행령

신설

제11조의6 (침해사고대응을 위한 금융위원회의 업무)

1. [침해사고대책본부]운영, [침해사고대응기관] 지정
2. 침해사고조사, 원인파악, 정보제공 등 협조 요청
3. **침해사고에 이용되는 접속경로 등 차단 요청**
4. 금융회사가 이용중인 SW중 침해사고와 관련 있는 SW제작사에 보안취약점 수정/재배포 요청

신설

제11조의7 (침해사고의 대응 절차 · 방법 등)

1. 침해사고대응기관 설치/지정/기능 등에 관한 사항
2. 발생보고/전파체계/사고예방을 위한 정보공유체계 마련에 관한 사항
3. 금감원장/대응기관이 사고원인분석, 피해확산방지를 위하여 긴급조치에 관한 사항
4. 침해사고대응을 위한 비상계획/훈련

발송일
2013. 08

개인정보 업종별 가이드라인 ①

금융분야 개인정보보호가이드라인

원문보기

금융기관 개인정보보호 가이드라인

[적용대상] 금융기관

[발간부처] 금융위원회, 금융감독원/
행정자치부 공동발간

[관련법] 신용정보법,
전자금융거래법 & 개인정보보호법

[업종상 특수개인정보] 개인신용정보

· 업종별 가이드라인은 무엇인가?
행정자치부가 (각각의 업종별로) 관련정부기관과 함께 공동발간한 개인정보보호법 관련 행정지도서임

· 가이드라인은 법적으로 강제력이 있는가?
원칙상 법적으로 강제력이 있는 것은 아니나 가이드라인을 준수하면 법을 준수했다고 판단
실제는 강제력 있으며 미준수시 처벌받음

[개인정보보호법]과 [금융분야 개별법] 충돌시 어느 법을 적용하는가?

'개별법'을 먼저 적용함

개인신용정보는 신용정보법 우선적용, 이외 개인정보는 개인정보보호법 우선적용

[신용정보법]상 규정된 개인신용정보는 무엇인가?
금융거래 등 상거래시 거래상대방 개인의 신용도판단을 위한 정보

식별정보
성명, 주소,
주민번호,
외국인등록번호, 여권번호,
성별, 국적, 직업 등

신용도정보
연체,부도,대위변제,
대지급, 거짓, 속임수,
신용질서 문란행위 관련
금액발생/해소시기

신용거래능력 판단정보
재산, 채무, 소득총액,
납세실적

유사정보
법원심판/결정,
조세, 요금체납 등

고유식별정보 내부망 저장시 암호화는 개인정보보호법규정을 따름
▶ DB내 고유식별정보는 [위험도분석]을 거쳐 암호화여부 결정

[개인정보의 안전성 확보조치]관련 금융기관 3대법 비교

금융기관은

- 개인신용정보는 신용정보법 및 전자금융거래법 준수
- 개인신용정보중 고유식별정보 암호화는 개인정보보호법 준수
- 개인신용정보 외의 개인정보는 개인정보보호법 준수
- 개인신용정보와 그 밖의 개인정보를 같은 시스템으로 통합관리하면서 신용도판단(신용정보법 적용), 전자금융거래(전자금융거래법 적용), 마케팅(개인정보보호법 적용) 등 다목적으로 이용시에는 세 법 모두 준수
- 세 법이 사실상 일치할 경우 한 법만 준수해도 세 법을 다 준수한 것으로 간주

<table>
<tr><th>구분</th><th>개인정보보호법고시
개인정보의 안전성 확보조치 기준 고시</th><th>신용정보법
신용정보업감독규정</th><th>전자금융거래법
전자금융감독규정</th><th>기술적 보호조치</th></tr>
<tr><td rowspan="3">접근권한관리</td><td colspan="3">업무별로 접근권한 최소, 차등부여
(개 〈개인정보처리시스템〉 접근권한, 신 신용정보처리시스템 접근권한, 전 전산자료접근권한)</td><td rowspan="3">· DB방화벽
DB-i
· IPS/IDS</td></tr>
<tr><td>개인정보취급자별 1계정</td><td>-</td><td>상이 계정공동사용이 불가피할시 개인별사용내역 관리</td></tr>
<tr><td colspan="3">인사이동시 지체없이 접근권한변경 (개, 신은 변경내역 3년보관 규정 존재)</td></tr>
</table>

사실상 일치

<table>
<tr><th>구분</th><th>개인정보보호법고시
개인정보의 안전성 확보조치 기준 고시</th><th>신용정보법
신용정보업감독규정</th><th>전자금융거래법
전자금융감독규정</th><th>기술적 보호조치</th></tr>
<tr><td rowspan="3">접근통제시스템</td><td>외부접속시 VPN,
전용선 등 적용</td><td>-</td><td>정보보호시스템을 우회한
외부통신망 접속금지</td><td rowspan="3">· DB방화벽
DB-i
· VPN</td></tr>
<tr><td colspan="2">개인정보가 비권한자에게 유출되지 않도록
시스템 및 컴퓨터 조치</td><td></td></tr>
<tr><td colspan="3">[접근통제시스템] 설치 운영(침입차단시스템 및 침입탐지시스템 포함)</td></tr>
</table>

사실상 일치

(뒷장에서 계속)

[개인정보의 안전성 확보조치]관련 금융기관 3대법 비교 (앞장에서 계속)

구분	개인정보보호법고시 개인정보의 안전성 확보조치 기준 고시	신용정보법 신용정보업감독규정	전자금융거래법 전자금융감독규정	기술적 보호조치
암호화	고유식별정보 내부망 저장시 암호화는 개인정보보호법규정에 따름 ▶ DB내 고유식별정보는 [위험도분석]을 거쳐 암호화여부 결정			·PC, 보조저장매체 내 개인정보 암호화 Privacy-i ·서버내 개인정보 암호화 Server-i ·DB암호화
	[대상] 고유식별정보, 비밀번호, 바이오정보	[대상] ·본인인증정보 (패스워드, 생체정보) ·개인신용정보	[대상] 전자금융거래정보, 비밀번호, 거래로그	
	고유식별정보를 PC/인터넷구간/DMZ구간/ 보조저장매체 저장시 암호화	개인신용정보 PC저장시 암호화	거래로그 DMZ구간내 저장시 암호화	
	송수신시 암호화 (개 정보통신망송수신시 암호화, 신 송수신시 보안서버 등을 통해 암호화, 전 전자금융거래는 암호화통신 적용)			
	일방향 암호화 (개 비밀번호, 신 본인인증정보)		비밀번호는 암호화보관, 조회불가하게 조치	
	안전한 암호화알고리즘 적용		국가기관이 평가·인증한 정보보호제품사용	

일부내용 상이

구분	개인정보보호법고시 개인정보의 안전성 확보조치 기준 고시	신용정보법 신용정보업감독규정	전자금융거래법 전자금융감독규정	기술적 보호조치
접속기록	[〈개인정보처리시스템〉] 접속기록 6개월이상 보관	[개인신용정보처리시스템] 접속기록저장 월1회 이상 확인감독	단말기를 통한 이용자정보조회시 **사용자, 사용일시, 변경조회내용, 접속방법을** 정보처리시스템에 자동 기록 / 1년 이상 보존	접속기록저장 / 로그위변조방지 스토리지탑재 DB-i
	-	[개인신용정보]에 대한 조회자신원, 조회일시, 대상정보, 목적, 용도 등을 기록관리	[정보처리시스템] 가동기록 1년이상 보존 (접속일시, 접속자, 접근자 / 접근을 확인할 수 있는 기록, 전산자료 사용일시, 사용자 / 자료 내용 확인기록, 사용자로그인, 액세스로그 등)	
	접속기록위변조방지			

사실상 일치

(뒷장에서 계속)

[개인정보의 안전성 확보조치]관련 금융기관 3대법 비교 (앞장에서 계속)

구분	개인정보보호법고시 개인정보의 안전성 확보조치 기준 고시	신용정보법 신용정보업감독규정	전자금융거래법 전자금융감독규정	기술적 보호조치
물리적 보호 조치	· 개인정보 물리적 보관소 출입통제	· 침입방지, 출입자통제	· 전산실 건물 경비원통제/ 출입통제 · 무인감시카메라/출입기록 시스템 설치 등 보안조치	경비원, 시건장치, CCTV, 출입기록시스템
	상이 서류, 보조저장매체는 잠금장치있는 안전한 장소에 보관	-	-	개인정보출력물 현황관리 Privacy-i

사실상 일치

구분	개인정보보호법고시 개인정보의 안전성 확보조치 기준 고시	신용정보법 신용정보업감독규정	전자금융거래법 전자금융감독규정'	기술적 보호조치
내부 관리 계획	· [내부관리계획] 수립/시행 · 상이 [내부관리계획] 수정이력 관리	[내부관리규정] 마련	· [전자금융거래 안전성확보 계획] 수립 · [정보기술부문계획] 매년 수립 · 전산자료,시스템, 해킹 등 [분야별보호대책] 수립	
비밀 번호	[작성규칙] 수립			
보안 프로 그램	· 백신설치, 자동/일1회이상 업데이트 · 보안업데이트공지시 즉시 업데이트		· 악성코드대책수립 · 악성코드치료프로그램 최신상태 유지 · 중요단말기는 감염여부 매일 점검	· 백신 · 악성코드 감염사이트 접속차단 WebKeeper

주요내용 사실상 일치

이외 개인신용정보에 적용되는 안전성 확보조치

개인신용정보 파기

언제 파기하는가?	어떻게 파기하는가?	기술적 보호조치
· 불필요하게 되었을 때는 지체 없이 (5일 이내) 파기 · 법령상 잔여보유기간이 있는 경우에는 다른 개인정보와 분리하여 저장/관리	· 신용정보 파기절차/방법을 공시 · 전자적파일은 복구 or 재생되지 아니하도록 파기 · 종이문서는 분기/반기단위로 별도점검 및 파기절차 마련	· Privacy-i · 디가우저 · 파쇄기

유출시 통지

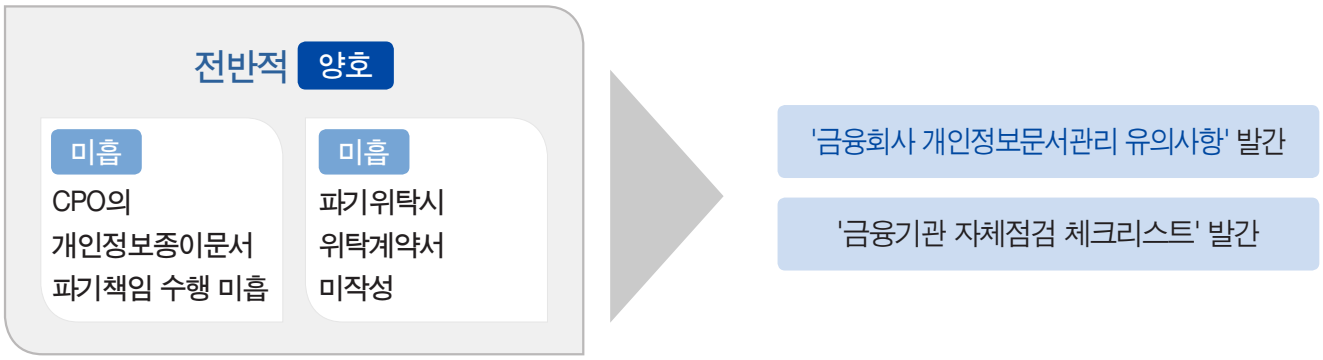
유출시 무엇을 통지하는가?	어디에 신고해야 하는가?	기술적 보호조치
개인정보 유출시 통지사항 1) 개인정보항목 2) 유출시점/경위 3) 피해 최소화 방법 4) 대응조치/피해구제절차 5) 신고 접수처	1만건 이상의 개인신용정보가 유출된 경우 1) 정보주체통지 2) 행자부/인터넷진흥원에 신고(사고발생 5일내) 3) 금융감독원 개인정보보호 담당부서에 신고 4) 금융기관검사/제재에관한규정 제41조(금융사고), 전자금융감독규정 제73조(사고보고)에 해당시 금융위원회 or 금융감독원 보고	[네트워크DLP] Mail-i [엔드포인트 DLP] Privacy-i 유출내역 기록,경보

발송일
2013. 08

금융감독원

[금융회사 개인정보문서관리 유의사항] 발간

금융감독원 IT감독국 개인정보보호TF가 2013년 6월 28일 ~ 7월 12일
165개 금융기관(은행, 증권, 보험, 카드)대상으로 개인정보 종이문서 관리실태조사 실시



'금융기관 자체점검 체크리스트' 내용

개인정보종이문서의 안전관리

체크리스트 규정	전제조건	기술적 보호조치
[내부관리계획]에 개인정보종이문서의 '안전성확보조치' 고려 ▶위반시 3천만원 이하 과태료	· 개인정보종이문서의 탄생시점 즉 출력시점부터 이력관리를 잘해야 한다 · 금융기관 내에서 어떤 개인정보를 얼마나 출력했는지 기록/추적해야 한다	개인정보출력물 현황관리 Privacy-i
[개인정보처리방침]에 개인정보종이문서의 '안전성확보조치' 고려, 홈페이지에 공개 ▶위반시 1천만원 이하 과태료		
개인정보종이문서를 잠금장치 있는 안전한 장소에 보관 ▶위반시 3천만원 이하 과태료 ▶개인정보유출시 2년 이하 징역, 1천만원 이하 벌금		

개인정보종이문서의 파기절차

체크리스트 규정	전제조건	기술적 보호조치
'개인정보'가 불필요하게 되었을 때 즉시 파기 **개인정보종이문서**는 분기/반기 단위로 점검/파기 ▶위반시 3천만원 이하 과태료	· CPO책임하에 **개인정보종이문서**의 유효기간을 전사적으로 파악해야 함 · 출력시점부터 (상부결재 등의 방식으로) 개인정보출력물현황/ 유효기간을 기록해야 함	개인정보출력물 결재/ 유효기간 기록 Privacy-i
개인정보출력물은 파쇄/소각으로 복구재생 안되도록 완전파기 ▶위반시 3천만원 이하 과태료		
개인정보종이문서 파기사항 기록관리		
개인정보종이문서의 파기를 CPO책임하에 수행 · CPO는 **개인정보종이문서** 파기에 대한 최종 의사결정권한/책임자임		
CPO가 **개인정보종이문서**파기결과확인 · 금융기관 지점장/지점의 파기책임자가 확인 ▶ CPO에게 보고		

개인정보종이문서 위탁관리

체크리스트 규정
개인정보종이문서 파기를 외부위탁시 문서에 의하여 함 ▶ 위반시 1천만원 이하 과태료
파기위탁시 위탁업무/수탁자를 (홈페이지등에) 공개 ▶ 위반시 1천만원 이하 과태료
파기수탁자선정시 인력, 시설, 기술 등을 종합적으로 고려
파기수탁자에게 개인정보보호교육 실시
파기수탁자가 개인정보를 안전하게 처리하도록 관리감독

발송일
2013. 08

종합대책! 2년만에 다시 등장하다

[금융전산 보안강화종합대책] 2013년 11월 23일부터 시행

원문보기

사이버공격은 대형화/지능화, 기존 대응체계는 무력화

이제 금융보안의 패러다임이 바뀐다

패러다임변화① 금융보안예산은 비용이 아니라 투자

패러다임변화② 금융회사가 자율적으로 보안강화

→ CISO를 CIO와 직무분리, 내부제재권한 강화, 보안인력 사기진작대책 마련으로
금융회사 내 보안조직 위상을 높임으로써 자체적 보안역량강화, 자율적 내부규제강화

핵심사항 보기

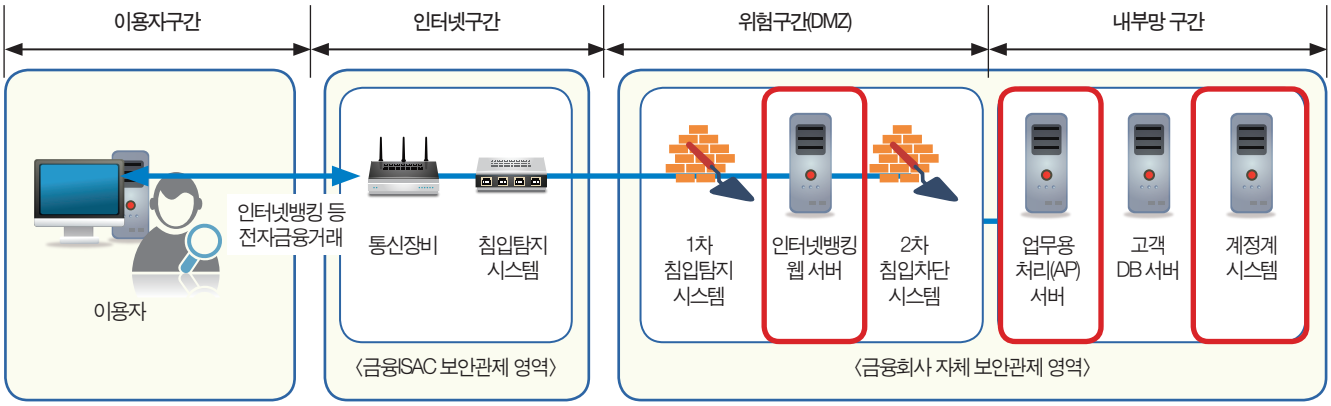
CISO 역할 및 독립성 강화

핵심사항	현재 문제점을	향후 이렇게 개선
CIO-CISO 겸직 금지	· 업무경계모호로 책임불분명 · IT보안보다 IT효율성이 우선되어 안전성 약화 · CISO는 권한에 비해 책임이 큼	· CISO전임제(겸직금지) 도입 (총자산 10조, 직원수 1,500명 이상 36개사대상) · 전임 CISO는 집행임원으로 지정 가능
전임CISO 임기보장	문책부담해소, 업무연속성 확보	부당한 인사상 불이익금지 및 최소임기보장
CISO산하 의사결정기구	IT 보안관련 의사결정기구 혼재	CISO하에 독립적 의사결정기구로 〈IT보안위원회〉운영
CISO 정책협의회	금융위는 CISO로 구성된 정책협의회를 매분기 개최	〈CISO 정책협의회〉의 법적 근거 마련

금융권보안전담조직 체계화

핵심사항	현재 문제점을	향후 이렇게 개선
보안컨트롤 타워는? 금융위원회!	금융결제원, 코스콤, 금융보안연구원간 업무중복	**금융위를 컨트롤타워로** 관련기관을 모아 [금융전산보안협의회]설치 (8월)
금융ISAC에 침해사고대응전담 상시조직 운영	사고발생시 초동조치/원인 분석/대응을 위한 상시전담조직 부재	**금융ISAC에 [침해사고대응전담반] 운영**
전금융권 대상 **이용자 → 웹서버 → 애플리케이션서버 → DB서버까지 실시간 모니터링** 체계 구축	금융ISAC과의 연계 저조 금융ISAC(infomation Share Analysis Center)이란? 금융결제원, 코스콤에서 운영하는 금융정보공유, 분석센터 금융결제원이 은행권을, 코스콤이 증권사를 담당한다. 각 회원사와 증권사와 연계하여 통합보안관제를 실시한다.	· **전 금융권실시간 모니터링**/악성코드, 보안취약점정보공유체계 구축 · 금융권보안관제기구의 설치근거마련/ **금융ISAC과 연계의무화**

〈금융권 침해대응 모니터링 체계〉



전산보안인력 사기진작

핵심사항	현재 문제점을	향후 이렇게 개선
CEO 책임하에 사기진작방안 마련	인사/성과평가 불리 보안업무 기피	**해외연수, 성과평가 가점, 금융보안 석사과정 학비지원, 정부 훈/포상 추천, 금융위원장 표창 수여**
보안담당자 **면책근거 마련**	사고시 금융회사 책임강화로 보안담당자고충 가중	**의무를 다한 경우 면책**

금융전산 내부통제 강화

핵심사항	현재 문제점을	향후 이렇게 개선
CEO 책임하에 취약점 점검/보완	동일취약점을 이용한 해킹발생	IT자산식별 → 취약점점검 후 조치계획 수립, 이행 여부를 CEO에 보고
非금융시스템까지 취약점점검/관제	보안상 취약점 존재	홈페이지/그룹웨어도 취약점 점검 의무화 (금융ISAC연계 권고)
운영자대상 접근통제 강화	운영자의 내부망 전산시스템 접근시 추가인증 미적용	· 운영자의 모든 전산시스템 접근시 ID/비밀번호 이외 추가인증 의무화(IC카드, OTP 등) · **계정 사용권한, 접근기록, 작업내역 중점관리, 상시통제** · 중요 단말기는 인터넷, 메일, 그룹웨어 접속금지
내부업무시스템 인터넷 접속차단	PMS로 악성코드 유포 (Patch Management System)	· 패치관리, 그룹웨어는 인터넷 접속차단 (외부파일전송시 수동다운로드후 검증) · 메일은 별도의 중계시스템으로 접속 · 각종 파일배포기능 통합관리
보안조직의 내부제재권한 강화	보안조직의 권한부족	· 정보보안조직은 임직원의 보안준수여부를 정기점검, **결과를 CISO, CEO에 보고** · **처벌근거를 금융회사 내규에 마련/시행**

금융보안 관리체계 인증제도 도입

핵심사항	현재 문제점을	향후 이렇게 개선
[인증제도]도입	평준화된 보안수준을 **회사규모에 따라 차별화**	· 매출 10조 및 직원수 1,500명 이상인 **36개사는** **금융보안 관리체계인증 의무화**(예상) · 인증획득시 **정보기술부문 실태평가 가점 부여 or 면제**

금융보안 전문인력 양성 및 교육 강화

핵심사항	현재 문제점을	향후 이렇게 개선
금융보안 전문 교육과정확대	교육 부족	금융보안연구원은 〈금융정보보호 교육센터〉 운영
임직원 보안교육 강화	전문인력 부족	연간 정보보호교육계획 수립/시행 (직원별 최소이수교육시간 운영)

금융권 공동 백업전용센터(제3백업센터) 구축

핵심사항	현재 문제점을	향후 이렇게 개선
공동 백업전용센터구축	전산센터와 백업센터에 DB삭제공격 발생시 동시파괴될 위험 존재 (은행DB삭제공격이 2011년, 2013년에 발생)	금융권 공동 백업전용센터를 지방에 지하/벙커로 구축

금융전산 위기대응능력 강화

핵심사항	현재 문제점을	향후 이렇게 개선
신종 사이버위협대비 모의훈련 강화	사이버공격은 다양화되는데 여전히 모의훈련은 디도스로만?	APT공격/악성코드 내부망침투 등을 대비하여 모의훈련시나리오 개선
재해복구센터 운영 등 복구체계 강화	영업점 단말기 등 대규모장애 대비 위기대응시나리오 미흡	재해복구센터전환시점 매뉴얼화, 긴급복구절차 마련, 영업점단말기 긴급복구파일 등 전산자원 확보
정전 대비 대응체계 강화	은행영업점 UPS보유율저조 (UPS: Uninterruptible Power Supply)	비상/이동발전기로 정전에 대비, UPS장비확보계획 마련

금융전산 망분리 의무화 및 가이드라인 배포

핵심사항	현재 문제점을	향후 이렇게 개선
망분리 의무화 및 가이드라인 배포	인터넷과 연결된 PC, 단말기가 악성코드에 감염	· 모든 금융회사 전산센터는 물리적 망분리 (2014년 12월까지) 본점, 영업점은 단계적망분리 (논리적망분리 가능) · 망분리 기획단계에서 금감원의 사전검토 · [망분리 가이드라인] 8월 배포

금융이용자보호강화

핵심사항	현재 문제점을	향후 이렇게 개선
FDS구축확대	카드사가 FDS 개별운영 FDS(Found Detection System) 전자금융거래시 단말기 정보, IP 주소, 거래내용을 분석/의심거래 탐지 / 차단시스템	FDS를 은행, 증권으로 확대 및 이상금융거래정보 공유체계 구축권고
금융회사 사칭 불법사이트 접속차단 (금융ISAC이 추진)	파밍, 스미싱 등 공격지능화	· [불법/유해사이트 차단시스템]으로 금융회사사칭 불법사이트 접속차단 *불법/유해사이트 차단시스템 : 해외전송구간을 모니터링하여 해외서버에서 제공하는 불법사이트차단 · 해외불법사이트 발견시 블랙리스트등록, 접속 즉시 차단
이용자 교육	사고예방 개인정보유출방지를 위한 이용자교육 미흡	영업점에서 유의사항 배포 및 온라인거래시 사고예방법 설명

금융전산부문 감독 및 검사 강화

핵심사항	현재 문제점을	향후 이렇게 개선
지주회사 및 IT자회사감독강화	3.20사태시 A지주그룹웨어, B중앙회 백신배포서버에 악성코드 삽입	· 지주사의 주력 자회사 검사시 **IT자회사도 연계검사** · 지주사와 자회사간 **위수탁계약시 책임관계명시**
전산사고 빈번한 금융회사 집중관리	금융회사의 사고재발을 위한 노력미흡	· **금융당국이 집중 점검/관리** · 사고시 지체없이 금융회사 홈페이지에 공시
6개월 업무정지의 제재기준 마련	전자금융거래법 업무정지규정 세부기준 부족	안전조치 위반시 업무정지(최대 6개월)규정의 세부기준 마련

금융회사의 자율적 보안노력 지원

핵심사항	현재 문제점을	향후 이렇게 개선
신기술 보안가이드	폰뱅킹, 무인점포 등의 보안미흡	[IT신기술접목 전자금융거래 보안가이드] 제공
중소형 금융회사 보안지원체계 마련	자율보안진단으로 보안강화 유도	자체진단을 위해 [금융 IT 보안수준진단 가이드라인]제공

발송일
2013. 05

5월22일 공포

[전자금융거래법 개정안] 2013년 11월 23일부터 시행

원문보기

핵심사항 1

제9조 1항 (금융회사의 책임)

① 금융회사는 다음 사고로 이용자에게 손해가 발생한 경우, 손해배상책임을 진다

기존
사고1 접근매체의 위조나 변조로 발생한 사고

기존
사고2 계약체결 or 거래지시의 전자적 전송이나 처리과정에서 발생한 사고

신설
사고3 전자금융거래를 위한 전자적 장치 or (정보통신망법에 따른) 정보통신망에 침입하여 거짓이나 그 밖의 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고

- 전자적 장치: 현금자동지급기, 자동입출금기, 지급용단말기, 컴퓨터, 전화기, 휴대폰 등 정보전송 및 처리장치
- 접근매체: 현금카드, 신용카드, OTP, 공인인증서, 이용자ID, 비밀번호, 생체정보 등 전자금융거래 및 인증을 위한 정보

2014년 1월부터 해킹사고시 금융회사가 배상책임을 져야 함

제9조 2항

② 다음 경우 책임의 전부 or 일부를 이용자에게 부담하게 할 수 있다.

1. 이용자의 고의/과실로 사고발생시, 그 책임을 이용자가 진다는 약정을 체결한 경우
2. 금융회사가 보안절차를 수립/철저히 준수하는 등 합리적인 주의의무를 다한 경우

핵심사항 2

제21조 4항 (정보기술부문계획 수립/제출)

금융회사는

신설
매년 IT부문계획을 수립하여 CEO의 확인/서명을 받아 금융위원회에 제출해야 한다

대통령령에서 대상 금융기관, 전자금융업자 구체화 예정

보안은 CEO가 책임져야 하는 사항임

핵심사항 3

제21조 3항 (전자금융기반시설에 대한 취약점 분석/평가)

금융회사는

신설

① 다음 사항에 대하여 취약점분석 · 평가를 실시하여 금융위에 결과보고
전자금융기반시설의 IT부문조직, 시설, **내부통제, 전자적장치, 접근매체 전자금융거래 유지를 위한 침해사고 대응조치**

▶ 전자금융거래에 이용되는 정보처리시스템 / 정보통신망

위반시 과태료
최대 2천만원

신설

② 금융위가 ①항의 결과에 대한 **이행실태점검 및 보완조치**를 실시할 수 있다

▶ 대통령령에서 구체화예정

핵심사항 4

제21조 4~6항 (전자적 침해행위 금지 및 침해사고 대응)

금융회사는

신설

제21조 4항 (전자적 침해행위의 금지)

▶ 전자적침해행위 (해킹, 바이러스, 논리/메일폭탄, 서비스거부, 고출력전자기파 등)으로 전자금융기반시설을 공격하는 행위

위반시 형사처벌
(7년이하 징역 or
5천만원 이하 벌금)

신설

제21조 5항 (침해사고의 통지 등)

① **침해사고** 발생시 금융위원회에 지체없이 통지해야 한다

▶ 침해사고 : 전자적 침해행위로 인하여 전자금융기반시설이 교란, 마비되는 사고

위반시 과태료
(2천만원이하)

신설

제21조 6항 (침해사고의 대응)

① 금융위는 침해사고에 대한 정보수집 전파, 예보 경보, 긴급조치를 수행한다

▶ 대통령령에서 구체화 예정

핵심사항 5

제40조 4~6항(전자금융보조업자 조사)

금융회사는

▶ VAN사업자 등 금융기관 or 전자금융업자 업무의 일부를 대행하는 업무를 행하는 자 or 결제중계시스템 운영자

신설

제40조 4~6항 (**전자금융보조업자** 조사강화)

④ 금감원장은 보조업자가 자료를 미제출/부실제출시 조사할 수 있다

⑤ 금감원장은 보조업자에게 진술서, 장부, 서류, 물건제출 관계인 출석을 요청할 수 있다

전자금융보조업자는 평상시 사내정보 기록관리를 시행해야함

전자금융거래법 조항보기

조문 및 핵심사항	주요내용	기술적 보호조치
6조 접근매체 선정과 사용 및 관리	① 접근매체를 선정하여 사용/ 관리하고 이용자의 신원, 권한 및 거래지시의 내용 등을 확인해야 한다 ② 접근매체발급시 사용자신청이 있는 경우에 한하여 본인확인 후에 발급하여야 한다 **처벌** 위반시 영업정지(최대 6개월)	
8조 오류의 정정 등	① 이용자는 전자금융거래에 오류발견시 정정을 요구할 수 있다 ② 금융회사는 정정요구를 받으면 즉시 처리 후 2주내에 오류원인과 처리결과를 이용자에게 알려야 한다 ③ 금융회사는 스스로 전자금융거래오류 발견시 즉시 조사/처리후 2주 이내에 오류의 원인과 처리 결과를 이용자에게 알려야 한다 **처벌** 위반시 영업정지(최대 6개월)	
16조 전자화폐 발행, 사용, 환금	① 전자화폐 발행시 접근매체에 식별번호를 부여하고 그 식별번호와 이용자의 실지명의/예금계좌를 연결하여 관리하여야 한다 **처벌** 위반시 영업정지(최대 6개월)	
21조 안전성 확보의무	① 전자금융거래의 안전성을 위하여 주의해야 함 ② 전자적 전송을 위한 인력, 시설, 전자적장치, 소요경비에 관하여 금융위원회기준을 준수한다 **처벌** 위반시 영업정지(최대 6개월)	

(뒷장에서 계속)

전자금융거래법 조항보기 (앞장에서 계속)

조문 및 핵심사항	주요내용	기술적 보호조치
21조 4항 **임원급 CSO지정**	② 대통령령으로 정하는 금융기관 or 전자금융업자는 CISO를 임원으로 지정한다	
22조 **전자금융** **거래기록** **생성 / 보존**	① 전자금융거래기록 생성, 최대 5년 보존 1) **5년** (보조업자는 3년) 전자금융거래의 종류, 금액, 상대방의 정보, 거래일시, 전자적장치의 종류/식별정보, 거래계좌명칭/번호, 금융회사가 받은 수수료, 지급인의 출금동의사항, 전자적장치의 접속기록, 신청 및 조건의 변경사항, 건당거래액 1만원 초과인 전자금융거래기록 2) **1년** 건당거래액 1만원 이하 전자금융거래 기록, 거래승인기록 ② 전자금융거래기록을 서면, 마이크로필름, 디스크/자기테이프 등으로 보존 [전자거래기본법 5조 1항에 따른 전자문서 보존시 요건] 1. 내용을 열람할 수 있을 것 2. 작성/송수신시의 형태 or 재현가능한 형태로 보존될 것 3. 작성자, 수신자, 송신 · 수신일시가 보존되어 있을 것	***DB-i*** DB접속기록보존 / 위변조방지 ***Mail-i*** 네트워크메시지 보존/위변조방지
25조 **약관제정 / 변경**	① 전자금융거래약관 제정/변경시 미리 금융위원회에 보고해야 한다 ② 금융위는 금융회사에 전자금융거래 약관변경을 권고할 수 있다	
27조 **분쟁처리 및 조정**	① 이용자가 전자금융거래에서 입은 손해에 대하여 손해배상절차를 마련 하여야 한다 ② 이용자는 손해배상, 분쟁조정을 신청할 수 있다 (금감원 or 소비자보호원을 거쳐)	
39조 **감독 및 검사**	① 금감원은 금융위의 지시를 받아 이 법의 준수여부를 감독한다 ② 금감원장은 필요시 금융회사에게 업무보고를 요청할 수 있다 ③ 금감원장은 금융회사의 전자금융업무를 검사하고, 필요시 자료제출, 출석을 요청할 수 있다 ④ 3항에 따라 검사를 하는 자는 권한을 표시하는 증표를 관계인에게 보여야 한다 ⑤ 금감원장은 3항에 따라 검사시, 결과를 금융위에 보고하여야 한다. ⑥ **금융위는 금융회사가 이 법을 위반한 경우 금감원장의 건의에 따라 다음 조치를 할 수 있다.** **1. 위반행위에 대한 시정명령** **2. 주의 or 경고** **3. 임원과 직원에 대한 주의, 경고 or 문책의 요구** **4. 임원의 해임권고 or 직무정지의 요구**	
40조 **금융기관등의** **제휴 or** **외부주문에 대한** **감독 및 검사**	① 보조업자와 제휴,계약체결/변경시(보조업자간계약포함) 안전성확보를 위하여 금융위 기준을 준수 ② 금융위는 계약내용의 시정 or 보완을 지시할 수 있다 ③ 금감원장은 보조업자에 대한 자료제출을 요구할 수 있다	

05

보건복지부 산하기관

발송일
2014. 09

개인정보 업종별 가이드라인④

의료기관 개인정보보호 가이드라인

원문보기

주민번호 신규수집 금지 관련
2015년 2월 6일 계도기간 종료 후 의료기관은 어떤 처벌을 받게되나?

주민번호 수집 · 이용시	주민번호 유출시	개인정보보호법 위반시
3천만원 과태료	과징금 5억	대표이사 · 임원 징계

보유 중인 주민번호는 2016.08.07까지 파기해야함

주민번호수집이용이 가능한 **진료목적업무**(개인정보수집시 동의 불필요)

진료기록부
[수집항목]
주민번호, 성명, 주소, 병력, 가족력, 주된 증상, 진단결과, 치료내용, 진료일시분

조산기록부
[수집항목]
주민번호, 성명, 주소, 소견, 분만 횟수/정보/장소/일시분, 산아성별/생사유무/부속물소견, 산후건강진단

환자명부
[수집항목]
주민번호, 성명, 주소, 연락처

처방전
[수집항목]
주민번호, 성명, 의료기관명, 처방의약품정보, 처방의료인정보, 조제약사성명

검사소견서
[수집항목]
주민번호, 성명, 의사면허번호, 소견인성명, 질병검사소견

방사선사진 / 소견서
[수집항목]
주민번호, 성명, 의사면허번호, 소견인성명, 방사선사진소견

진단서
[수집항목]
주민번호, 성명, 주소, 병명, 치료소견, 진단연월일

사망진단서
[수집항목]
주민번호, 성명, 주소, 성별, 실제생년월일, 발병/사망일시, 사망장소/원인, 사망의 종류, 의사성명, 면허번호

감염병환자신고서
[수집항목]
주민번호, 성명, 주소, 연락처, 직업, 성별, 감염병명, 발병일

응급환자진료의뢰서
[수집항목]
주민번호, 성명, 보호자성명, 주소, 연락처, 응급처치상황

특정수혈부작용신고서
[수집항목]
주민번호, 성명, 주소, 연락처, 혈액형, 내원시 질환명, 수혈기관명, 수혈전 검사결과, 수혈부작용 진단검사결과 등

헌혈경력 / 검사결과 조회서
[수집항목]
주민번호, 성명

헌혈증교부시 본인확인
[수집항목]
주민번호, 성명

수혈자내역서
[수집항목]
주민번호, 성명, 주소, 수혈일, 혈액형, 수혈량, 헌혈증번호

주민번호수집이용이 불가능한 **진료목적업무**(개인정보수집시 동의 불필요)

X 간호기록부
[수집항목]
체온, 맥박, 호흡, 혈압, 투약, 섭취/배설물, 처치/간호

X 수술기록부
[수집항목]
성명, 수술명, 수술기록

X 출생증명서
[수집항목]
출생아부모생년월일, 성명, 주소, 출생장소, 일시,
임신기간, 다태, 출생아성별/성명, 신체/건강상황

X 사산(사태)증명서
[수집항목]
사산아부모생년월일, 성명, 주소, 사산장소, 일시,
사산(사태)의종류, 원인

X 뇌사추정자 신고서
[수집항목]
뇌사추정자생년월일, 성명, 주소, 뇌사추정자상태/발생원인

X 헌혈증
[수집항목]
생년월일, 성명

진료신청 예약 수납업무 중 주민번호수집이용 가능 VS 불가능

(진료목적업무이므로 개인정보수집시 동의 불필요)

O 내원
[수집항목]
주민번호, 성명,주소,연락처,진료과목,환자등록번호 등

X 예약확인문자 발송
[수집항목]
생년월일, 성명, 주소, 연락처

1차 예방접종 후
2차 접종안내문자는
〈진료목적〉업무

O 인터넷/전화 진료예약
건강보험가입/건강검진대상여부 확인이 필요한 경우 수집가능

[수집항목]
주민번호, 성명,주소,연락처,진료과목,환자등록번호 등

X 병원이전 / 휴업관련 정보전달
[수집항목]
생년월일, 성명, 주소, 연락처, 진료과목 등

O 요양급여의뢰서
의사가 작성한 종합전문 요양기관 진료요청서

[수집항목]
주민번호, 가입자 · 세대주 · 환자성명, 주소, 연락처,
건강보험증번호, 진료기간, 환자상태, 진료소견 등

X 진료비수납
[수집항목]
성명, 진료비, 카드사, 카드번호

〈홍보목적〉업무 : 개인정보수집시 동의 필요

X 홈페이지 회원가입 및 관리, 전체회원대상 홍보문자 등

[수집항목]
생년월일, 성명, 주소, 연락처

전체회원대상 예방접종안내문자는
〈홍보목적〉업무

의료기관 가이드라인

[적용대상]
의원급의료기관, 병원급의료기관, 조산원

[발간부처]
보건복지부/행정자치부 공동발간

[업종상 특수개인정보]
의료법상 규정된 〈진료정보〉

[관련법]

- 의료법
- 건강검진 기본법
- 암관리법
- 혈액관리법
- 감염병의 예방 및 관리에 관한 법률
- 응급의료에 관한 법률 등

⊕ 개인정보보호법

· 업종별 가이드라인은 무엇인가?
행정자치부가 (각각의 업종별로) 관련정부기관과 함께 공동발간한 개인정보보호법 관련 행정지도서임

· 가이드라인은 법적으로 강제력이 있는가?
원칙상 법적으로 강제력이 있는 것은 아니나 가이드라인을 준수하면 법을 준수했다고 판단
실제는 강제력 있으며 미준수시 처벌받을 수 있음

의료기관은 지금 무엇을 해야 하는가?

[의료기관가이드라인] 내 개인정보보호규정		기술적·관리적 보호조치
의료기관은 환자의 건강상태, 신체적 특징, 병력 등 민감정보, 주민번호 등 고유식별정보, 그 밖에 신용카드번호, 통장계좌번호, 근로정보, 개인영상정보 등 다양한 개인정보를 처리하고 있음 - 가이드라인 3p	개인정보취급자의 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	PC(정규직, 비정규직 망라) 서버, DB까지 전사적 **개인정보현황분석 실시** (특히 2015년엔 주민번호가 중요)
병원정보시스템, OCS, EMR, PACS, LIS, 건강검진시스템, 병원홈페이지 등 〈개인정보처리시스템〉에 사용자/직무/그룹/역할별로 화면/메뉴/버튼(읽기, 쓰기, 출력, 다운로드 등) 단위의 상세 접근권한을 설계하고 적용해야 함 - 가이드라인 77p	〈개인정보처리시스템〉 접속방법은 의사, 간호사 등이 병원정보시스템 등 응용시스템을 통하여 접속하는 방법, DB관리자 등이 DB접속 툴을 이용하여 〈개인정보처리시스템〉에 접속하는 방법 등 다양한 방법이 존재하므로, 각 환경에 맞도록 접속기록을 남겨야 함 - 가이드라인 92p	응용시스템(=애플리케이션)도 개인정보처리시스템이므로 **접근권한관리 및 접속기록저장**
개인정보다운로드 권한의 경우, 다운로드 받은 파일에 의한 대량 개인정보유출이 가능하므로 권한 최소화 - 가이드라인 78p	업무용 컴퓨터에 고유식별정보 등 개인정보 저장시 분실, 고의, 실수, 악성코드 감염 등 다양한 위협요인에 따른 개인정보 유출위험이 매우 높으므로, 업무용 컴퓨터 내 개인정보 최소화 - 가이드라인 89p	의료기관은 보유기간 경과, 개인정보의 처리 목적 달성 등 개인정보가 불필요하게 되었을 때 지체없이 개인정보를 파기하고, 복구 or 재생되지 아니하도록 조치해야한다. - 가이드라인 96p	**전사적 개인정보검출 및 복구or 재생되지 않도록 파기**

의료법상의 〈진료정보〉란 무엇인가?

의료기관 개인정보보호 가이드라인 1p '용어의 정의'
〈진료목적〉으로 수집, 처리하는 개인정보가 포함된 정보로
진료기록부, 수술기록부, 조산기록부, 환자명부 등으로 관리되는 정보임
(주민번호, 성명, 주소, 연락처 등 포함)

〈진료목적〉의 범위는 어떻게 되는가?

예약, 진단, 검사, 치료, 수납 / 예약확인 문자발송, 검사결과 통보 / 병원이전 및 휴업관련 정보전달

〈진료정보〉에 적용되는 법은 무엇인가?

〈의료법〉과 〈개인정보보호법〉 모두 적용 (두법이 충돌할 경우〈의료법〉 우선 적용)

의료법 우선 적용

〈진료정보〉는
수집, 이용시
동의받지 않아도 됨

개인정보보호법상〈안전성 확보조치〉적용

개인정보보호법고시 [개인정보의 안전성확보조치기준]
을 준수해야 함

〈진료정보〉의 보유기간은 어떻게 되는가? (의료법 시행규칙 제15조)

- **10년** 진료기록부, 수술기록부
- **5년** 환자명부, 검사소견기록, 방사선사진 및 그 소견서, 간호기록부
- **3년** 진단서 등의 부본 원본훼손에 대비하여 예비보관, 사무용으로 만든 원본과 동일한 내용의 문서 (개정안 신설)
- **2년** 처방전

보유기간이 끝나면?

보유기간 만료일로부터
5일이내
복구 불가능한 방식으로 파기

〈진료목적〉상 필요시
연장보관

보유기간 중에 진료정보가 필요없어지면?

처리목적달성
폐업
서비스폐지

필요없어진 날로부터
5일이내
복구 불가능한 방식으로 파기

의료기관 적용법 01 개인정보보호법

조항	규정	상세내용	기술적 보호조치
21조	개인정보파기	전자파일은 복구, 재생되지 않도록 삭제 종이는 파쇄, 소각	[PC] Privacy-i [서버] Server-i

의료기관 적용법 02 공공기관기록물관리법 (의료기관이 공공기관인 경우 적용)

조항	규정	상세내용	기술적 보호조치
27조	진료정보 현황파악	공공기관인 의료기관은 연 1회 이상 기록물평가심의위원회 구성 진료정보 현황파악 및 연장여부 결정	[PC] Privacy-i [서버] Server-i

27p [개인정보의 안전성 확보조치 기준] 규정 보기

의료기관은 **개인정보보호법고시 [개인정보의 안전성 확보조치 기준]**을 준수해야 함

발송일
2014. 01

개인정보 업종별 가이드라인③

사회복지시설 개인정보보호가이드라인

원문보기

〈의의〉 개인정보의 양, 중요도에 있어서는 압도적이나 규모가 작다는 이유로
본격규제를 받지 않아온 사회복지시설에 대한 가이드라인 발간

사회복지시설의 개인정보 현황은?

사회취약층 민감정보 대량보유

(법에 따른) 주민번호 수집, 처리기관

계좌번호, 카드번호, 재산, 소득정보 대량보유

자원봉사시스템으로 인하여 14세미만, 학생 고유식별번호 대량보유

사회복지통합관리망(행복e음)과 연계 29개 기관, 67종 개인정보에 접근가능

설립 근거법률만 25개! 사회복지시설수 (2011년 기준) 5,340개 시설수 급속증가 중!

부정수급적발, 복지강화를 위해 개인정보 대량연계추세
(사회취약층 민감정보+ 금융정보+주민번호 대량연계)

사회복지시설의 현실은?

1 (개별상담, 재가방문중인) 사회복지사들은 어떤 개인정보를 가지고 있는가? 이직시 개인정보파기가 이뤄지고 있는가?

2 전직원 PC에 고유식별정보, 금융정보, 민감정보가 있는 얼마 안되는 기관?

3 (개인정보가 유출되면) 복지대상인 사회취약층들은 어떤 충격을 입을까? 특히 소년소녀가장, 기초생활수급자/조손가정/입양가정 청소년들은? (그 피해에 비례하여 처벌됨)

4 행복e음의 정보가 복지시설 내 흘러다니고 있지는 않은가?

사회복지시설이 해야 하는 기술적 보호조치는?

전직원 PC, 서버내 개인정보를 검출, 현황파악, 파기, 암호화해야 함

어떤 개인정보를 출력해서 가지고 나갔는지 출력물이력관리를 해야 함

행복e음의 정보가 PC에 파일저장되지 못하도록 조치해야 함

PC정보가 USB로 복사, 저장되지 못하도록 조치해야 함

사회복지시설 개인정보보호 가이드라인

[적용대상] 사회복지시설

[발간부처] 보건복지부/행정자치부 공동발간

[업종상 특수개인정보]
사회취약층 민감정보, 중고등학생 고유식별정보, 재산 소득정보, 금융정보 등

[관련법]

- 사회복지사업법
- 기초노령연금법
- 노인복지법
- 장애인활동지원법
- 장애인복지법
- 장애인연금법
- 정신보건법
- 사회서비스이용 및 이용권관리에 관한 법
- 소득세법
- 법인세법 등

+ **개인정보 보호법**

· 업종별 가이드라인은 무엇인가?

행정자치부가 (각각의 업종별로) 관련정부기관과 함께 공동발간한 개인정보보호법 관련 행정지도서

· 가이드라인은 법적으로 강제력이 있는가?

원칙상 법적으로 강제력이 있는 것은 아니나 가이드라인을 준수하면 법을 준수했다고 판단

실제는 업종상 특수상황을 반영한 가장 구체적, 실제적 문서로 위반시 처벌받음

사회복지시설은 어디를 말하는가?

정의: 사회복지사업법 제2조에 따른 '사회복지사업' 시설

사회복지사업법 제2조의 사회복지사업 정의

총 25개 법률에 따른 보호 · 선도, 복지사업, 사회복지상담, 직업지원, 무료숙박, 지역사회복지, 의료복지, 재가복지, 사회복지관, 정신질환자/한센병력자 사회복귀사업 및 관련사업

예) 지역별 종합복지관, (실버타운 포함)노인시설, 장애인시설, 아동복지시설, 노숙인시설, 미혼모시설, (사회취약계층고용)착한가게, 착한기업, 정신요양시설, 에이즈결핵한센병시설, 성폭력상담센터 등

사회복지시설 설립근거법 25개

1. 국민기초생활 보장법 2. 아동복지법 3. 노인복지법 4. 장애인복지법 5. 한부모가족지원법 6. 영유아보육법
7. 성매매방지 및 피해자보호 등에 관한 법률 8. 정신보건법 9. 성폭력방지 및 피해자보호 등에 관한 법률
10. 입양특례법 11. 일제하 일본군위안부 피해자에 대한 생활안정지원 및 기념사업 등에 관한 법률 12. 사회복지공동모금회법
13. 장애인 · 노인 · 임산부 등의 편의증진 보장에 관한 법률 14. 가정폭력방지 및 피해자보호 등에 관한 법률
15. 농어촌주민의 보건복지증진을 위한 특별법 16. 식품기부 활성화에 관한 법률 17. 의료급여법 18. 기초노령연금법
19. 긴급복지지원법 20. 다문화가족지원법 21.장애인연금법 22. 장애인활동 지원에 관한 법률
23. 노숙인 등의 복지 및 자립지원에 관한 법률 24. 보호관찰 등에 관한 법률 25. 장애아동 복지지원법

사회복지시설이 수집, 처리하는 개인정보 종류

사회복지 통합관리망 (행복e음) 통합 · 연계

입소자 / 이용자(정기/수시이용자)

〈수집하는 개인정보〉
▶ (사회서비스이용 / 이용권관리법률에 따라)
주민번호, 계좌번호

〈처리하는 개인정보파일〉
개별상담카드, 독거노인방문일지, 노인일자리신청서,
장기요양급여제공일지, 배설관찰일지,
건강관리기록지, 투약관리기록지,
목욕급여제공기록지, 체위변경/욕창관찰기록지
▶업무과정에서 대량의 민감정보 생성

〈관련시스템〉
사회서비스 전자바우처시스템

자원봉사자

〈수집하는 개인정보〉
▶(사회복지사업법에 따라)
고유식별정보 (14세미만 학생 자원봉사자 정보 포함)

〈처리하는 개인정보파일〉 자원봉사증명서발급대장

〈관련시스템〉 VMS (사회복지봉사활동관리인증시스템)

후원자

〈수집하는 개인정보〉
▶(소득세법, 법인세법에 따라) 고유식별정보

〈관련시스템〉 CMS (Cash Management Service)

방문자

〈수집하는 개인정보〉
▶(사회복지사업법에 따라) 고유식별정보

근로자

노동부/행자부 발간 **원문보기**
[인사노무 개인정보보호가이드라인] 참조

반드시 사회복지시설내 개인정보를 검출, 분류해서 현황을 파악해야 함

복지 부정수급자 적발을 위해 사회복지통합관리망(행복e음)의 정보연계 강화, 29개기관 67종 개인정보연계

ex) 〈소득재산정보〉 4대특수직역연금, 기여금, 부동산종합공부 · 전월세정보, 건보료기준, 농업외소득, 이자소득 등
〈건강정보〉 산재, 장기요양등급, CT, MRI 정보, 전문장해진단, 정신병력, 유전병력 등
〈기타〉 노인일자리사업 참여자정보, 기초생활보장자정보 등

사회복지시설이 준수해야 하는 [개인정보의 안전성 확보조치]

개인정보보호법21조 파기

파기대상	어떻게 파기하는가?	기술적 보호조치
· 입소, 이용종료자의 개인정보파일 · 복지사, 봉사자가 가져간 개인정보인쇄물	· 전자적파일은 복구/재생되지 아니하도록 전문SW사용 · 종이문서는 소각, 파쇄	Privacy-i 전자파일 파기 출력물 이력관리

개인정보보호법 유출시 통지

유출시 무엇을 통지하는가?	어디에 신고해야 하는가	기술적 보호조치
개인정보 유출시 통지사항 1) 개인정보항목 2) 유출시점 / 경위 3) 피해 최소화 방법 4) 대응조치 / 피해구제절차 5) 신고 접수처	**1만건 이상의 개인정보가 유출된 경우** 1) 정보주체통지 2) 행자부/인터넷진흥원에 신고 (사고발생 5일내)	[네트워크DLP] Mail-i [엔드포인트DLP] Privacy-i } 개인정보 외부 유출내역 기록

수탁자감독 체크리스트

수탁자감독	수탁자 감독 체크리스트(총 14개 중 소만사 관련 9개 항목)	기술적 보호조치
업무 위탁시 수탁자의 기술적, 관리적 보호조치 현황 감독	④ 〈개인정보처리시스템〉 접근권한을 관리하고 있는가? ⑤ 비밀번호작성규칙을 수립하여 적용하고 있는가? ⑥ 접근통제시스템을 설치하여 운영하고 있는가? ⑧ 〈개인정보처리시스템〉 접속기록을 보관 · 관리하고 있는가?	DB-i, was-i 〈개인정보처리시스템〉 접근통제 접근권한관리, 비밀번호적용, 접속기록보관
	⑦ 개인정보를 암호화하고 있는가? ⑪ 개인정보의 안전보관을 위하여 물리적 접근방지조치를 하고있는가? ⑬ 개인정보취급과정에서 발생한 출력물/임시파일을 즉시 삭제하고 있는가? ⑭ 개인정보보호법령의 각종대장을 작성 · 관리 · 비치하고 있는가?	Privacy-i 개인정보 검출, 파기, 암호화 행자부 등록파일대장작성지원 출력물 이력관리 (물리적접근방지를 해야하는 출력물 목록관리가능)
	⑫ 재위탁하거나 위탁목적외로 개인정보를 이용하고 있는가?	Mail-i 네트워크를 통한 개인정보 외부전송 차단 / 기록 Privacy-i 출력물, USB를 통한 개인정보 외부전송 차단 / 기록

발송일
2014. 01

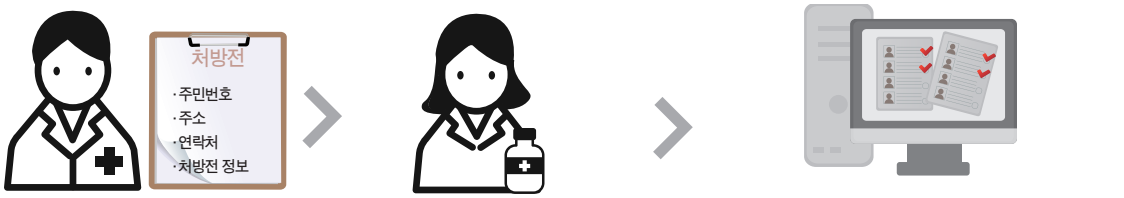
개인정보 업종별 가이드라인②

약국 개인정보보호 가이드라인

원문보기

〈의의〉 개인정보의 양, 중요도에 있어서는 압도적이나 규모가 작다는 이유로
본격규제를 받지 않아온 약국에 대한 가이드라인 발간

약국의 개인정보보호 현황은?



1 의사가 처방전 작성

2 약국 전산직원이 PC에 주민번호와 처방전 정보 입력

3 약국 전산직원이 PC에 주민번호와 처방전 정보 입력

개인정보를
단기계약직
전산직원이 담당

수면제, 피임약, 성형시술 등
민감정보가
주민번호와 함께 저장

처방전 2년, 보험급여청구처방전 3년, 요양급여청구정보 5년,
조제기록부는 5년, 마케팅목적은 동의받은 기간...
어떤 개인정보파일을
언제 파기해야 하는지 알 수 없음

약국은 지금 무엇을 해야 하는가?

시간제약사, 전산직원, 아르바이트 포함
상시근로자 5인 이상 약국의 3대 의무

1. 내부관리계획 수립 2.개인정보취급자 교육
3. 개인정보의 안전성 확보조치

〈약국관리프로그램〉상 개인정보가
파일로 복제, 방치되어있지 않는지
약국PC의 개인정보
주기적검출, 파기, 암호화

누가 어떤 개인정보를
출력했는지 알 수 있도록
약국PC
출력물 이력관리

개인정보를 복제,
유출하지않도록
약국PC
USB복사차단

개인정보가 인터넷으로
외부공개되지 않도록
약국PC의
P2P, 웹하드접속차단

[약국가이드라인] 내 개인정보보호규정

약국에서 근무하며 개인정보를 취급하는 자가
모두 개인정보취급자에 해당하므로
시간제 약사나 아르바이트생 관리와
감독을 철저히 해야 함

-가이드라인 52P

약국 PC에 엑셀(xls), PDF 등 전자문서파일형태로
주민번호를 저장할 경우
상용암호화SW로 암호화해야 함

-가이드라인 44P

유해사이트
차단프로그램 등을
사용하여 통제할 수 있음

-가이드라인 45P

약국 개인정보보호 가이드라인

[적용대상] 약국

[발간부처] 보건복지부/행정자치부 공동발간

[업종상 특수개인정보]
주민번호, 건강보험증번호,
질병정보, 투약정보, 요양급여비용

[관련법]

- 약사법
- 국민건강보험법
- 의료급여법
- 건강보험법 등

+ 개인정보 보호법

· 업종별 가이드라인은 무엇인가?
행정자치부가 (각각의 업종별로) 관련정부기관과 함께 공동발간한 개인정보보호법 관련 행정지도서임

· 가이드라인은 법적으로 강제력이 있는가?
원칙상 법적으로 강제력이 있는 것은 아니나 가이드라인을 준수하면 법을 준수했다고 판단
실제는 업종상 특수상황을 반영한 가장 구체적, 실제적 문서로 위반시 처벌받음

약국이 수집하는 개인정보종류

동의 필요없음	처방전	수집항목	성명, 주민번호, 주소, 연락처, 처방내용 (질병분류기호, 의료인성명 / 면허종류, 처방의약품, 발급연월일, 사용기간 등)
		정보형태	종이문서 or 전자파일
		수집방법	(약사법에 의해) 처방전 접수
		수집목적	건강보험급여청구
	조제정보 / 요양급여 청구정보	수집항목	성명, 주민번호, 가입자 성명, 건강보험증번호, 질병명, 요양급여비용의 내용, 본인부담금 및 비용청구액, 처방전의 처방내용
		정보형태	전자파일
		수집방법	처방전의 내용에 조제내역, 요양급여청구정보 추가 생성
		수집목적	조제관련 증빙자료 보존, 건강보험 요양급여청구
동의 필요함	고객 관리정보	수집항목	환자인적사항 등
		수집방법	고객정보 관리에 동의한 환자의 정보만 수집
		수집목적	DM, SMS 등을 통한 홍보 마케팅
	홈페이지 회원정보	수집항목	필수정보(성명, ID, 비밀번호), 선택정보(생년월일, 전화번호, 이메일, 관심정보 등) 주민번호가 있다면 '2014.08.07' 까지 파기
		수집방법	온라인상에서 회원가입 시 동의서를 받고 수집
		수집목적	홈페이지 회원관리

약국이 준수해야 하는 [개인정보의 안전성 확보조치]

PC에서 유해사이트접속차단

규정	기술적 보호조치
약국 PC는 (개인정보가 인터넷으로 외부공개되지 않도록) P2P, 웹하드접속을 차단해야 함	WebKeeper P2P, 웹하드 등 유해사이트접속차단 / 기록

파기

파기대상/유효기간	어떻게 파기하는가?	기술적 보호조치
· **처방전** 2년 · **보험급여청구처방전** 3년 · **요양급여청구정보** 5년 · **조제기록부** 5년 · **마케팅용고객정보** 동의받은 기간	· 전자적파일은 복구/재생되지 않도록 전문SW사용 · 종이문서는 소각, 파쇄	Privacy-i · 개인정보파일 유효기간 지정 · 복구재생불가하게 파기 · 출력물 이력관리

유출시 통지

유출시 무엇을 통지하는가?	어디에 신고해야 하는가	기술적 보호조치
개인정보 유출시 통지사항 1) 개인정보항목 2) 유출시점 / 경위 3) 피해 최소화 방법 4) 대응조치 / 피해구제절차 5) 신고 접수처	**1만건 이상 개인정보 유출시** 1) 정보주체통지 2) 행자부/인터넷진흥원에 신고 (사고발생 5일내)	[네트워크DLP] Mail-i [엔드포인트DLP] Privacy-i } 개인정보 외부 유출내역 기록

TEK&LAW

테크앤로법률사무소

SERVICES

1 지식재산권

2 해킹 침해사고 위기대응

3 개인정보 보호

4 ICT 비지니스 법률자문

5 게임 비지니스

서울시 종로구 종로1 15층 (종로1가 1번지, 교보생명빌딩)
T. 02-2010-8840 / *F.* 02-2010-8985

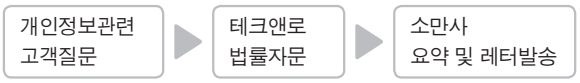
teknlaw@teknlaw.com
www.teknlaw.com
www.facebook.com/teknlaw

소만사 OX법률자문은 테크앤로와 함께 합니다

부록

OX 법률자문

소만사 고객님의 질문에 대하여
테크앤로 법률사무소에서 작성하신 법률자문서를
보시는 분의 편의를 위하여 소만사가 요약하였습니다



1. 고객님이 질문하신 시점의 법을 기반으로 작성하였습니다
   따라서 이후의 법률개정, 정책변경, 신규판례에 따라
   변화가 있을 수 있습니다
2. 테크앤로의 법률해석과 다른 견해도 존재할 수 있습니다
3. 보시는 분의 편의를 위하여 표현을 단순화하였습니다
   정확한 이해를 원하는 분께서는 변호사원문을 요청해주십시오

발송일
2014. 12

Q

우리단체는 매년 다양한 지역으로 봉사단원을 파견합니다

봉사활동 중 아픈 단원들은 그 지역에서 치료받습니다

단원들의 치료, 처방, 응급이송 등 진료정보는 봉사단에서 수집, 문서보관합니다

〈의료기관 개인정보보호 가이드라인〉에 따라 진료정보를 목적외 이용하거나 제 3자 제공하는 것은 금지된 줄로 압니다

병원이 아닌 봉사단체에서 봉사단원 진료정보를 수집/이용할 수 있나요?

A

O

조건

1 **봉사단원이 의료기관으로부터 진료정보를 〈직접 발급〉 받아야 함**

2 **봉사단체는 봉사단원에게** 개인정보보호법 제23조에 따라 일반 개인정보(이름, 생년월일, 주소 등) 외 **진료정보처리에 대한 〈별도동의〉를 받아야 함**

3 〈별도동의〉시 **진료정보종류, 보유 및 이용기간을 업무상 〈최소한으로 설정〉해야 함**
(기간만료시 봉사단원으로부터 진료정보 갱신)

근거1 단원 본인만 본인의 진료기록열람 및 사본발급 가능

의료법 시행규칙 제13조의2 4항 (기록열람 등의 요건)

환자가 본인 진료기록을 열람하거나 사본발급을 원하는 경우
본인임을 확인할 수 있는 신분증을 의료기관 개설자에게 제시해야 한다

근거2 진료정보는 민감정보이므로 일반개인정보와 별도동의를 받아야 함

개인정보보호법 제23조 (민감정보의 처리 제한)

개인정보처리자는 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보를 처리해서는 안 된다
다만, 다음 경우에는 그러하지 아니하다

1. 정보주체에게 개인정보처리 동의를 받은 경우
2. 법령에서 민감정보처리를 요구하거나 허용한 경우

근거3 최소한의 정보를 최소기간동안 수집/이용해야 함

개인정보보호법 제16조 (개인정보의 수집제한)

① 개인정보처리자는 개인정보 수집시 목적에 필요 최소한의 개인정보를 수집해야 한다
이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다
② 개인정보처리자는 정보주체동의를 받아 개인정보를 수집할 경우 필요 최소한의 정보 외 개인정보 수집에는 동의하지 않을 수 있다는 사실을 구체적으로 알리고 개인정보를 수집해야 한다
③ 개인정보처리자는 정보주체가 필요 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 or 서비스 제공을 거부해서는 안된다

개인정보보호법 제15조 2항 (개인정보의 수집/이용)

개인정보처리자는 개인정보수집 · 이용동의를 받을 때 다음 사항을 정보주체에게 알려야 한다

3. 개인정보의 보유/이용기간

봉사단체(일반기관포함)의 진료정보 이용기간관련 규정은 별도로 없음

발송일
2014. 10

Q

개인정보보호법에 따라
2014년 8월 7일부터
주민번호 사용이
불가능한 것으로 압니다

헌혈/혈액검사기록은
민감정보라서
핸드폰번호, 생년월일만 가지고
신원을 확인하기 어렵습니다

채혈 전 헌혈자 신원확인시, 채혈 후 헌혈증 발급시 주민번호를 요구할 수 있나요?

A

O

**혈액관리법 시행령 제10조의2에 따라
주민번호를 처리할 수 있는
업무입니다**

근거1

혈액관리법 시행령 제10조의2 (민감정보, 고유식별정보의 처리)

보건복지부장관(제10조에 따라 보건복지부장관의 권한 등을 위임 · 위탁받은 자 포함) or
혈액원은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우
개인정보 보호법 제23조에 따른 건강, 성생활에 관한 정보 (중간 생략)
같은 영 제19조제1호 or 제4호에 따른
주민번호 or 외국인등록번호가 포함된 자료를 처리할 수 있다

1 혈액관리업무 및 혈액원개설	**2 헌혈자 신원확인 및 건강진단**	3 채혈금지대상자 관리	4 혈액안전성확보
5 혈액사고발생시 조치	6 특정수혈부작용 조치	7 특정수혈부작용 및 채혈부작용 보상	8 혈액관리업무 기록작성
9 전자혈액관리업무 기록작성	10 품질관리검사	**11 헌혈증서 교부 및 환부**	12 혈액원 개설허가 및 취소

→ 2. 법 제7조에 따른 **헌혈자의 신원확인**, 건강진단 등에 관한 사무

혈액관리법 제7조 (헌혈자의 신원 확인, 건강진단 등)

① 혈액원은 채혈 전에 헌혈자 신원확인, 건강진단을 하여야 한다
② 혈액원은 감염병 환자, 건강기준에 미달하는 사람으로부터 채혈을 하여서는 아니 된다
③ 혈액원은 신원이 확실하지 아니하거나 신원 확인 요구에 따르지 아니하는 사람으로부터 채혈을 하여서는 아니 된다 (중간생략)
⑤ 혈액원은 채혈 전에 채혈금지대상 여부, 과거헌혈경력과 검사결과를 조회하여야 한다 다만, 천재지변, 긴급 수혈 등 보건복지부령으로 정하는 경우에는 그러하지 아니하다

→ 11. 법 제14조에 따른 **헌혈증서의 교부, 환부** 등에 관한 사무

혈액관리법 제14조 (헌혈증서의 발급, 수혈비용의 보상 등)

① 혈액원이 헌혈자로부터 헌혈을 받았을 때에는 보건복지부령으로 정하는 바에 따라 헌혈증서를 그 헌혈자에게 발급하여야 한다

근거2

개인정보보호법 제24조의2 (주민번호 처리 제한)

① 제24조제1항에도 불구하고 개인정보처리자는
다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민번호를 처리할 수 없다

1. 법령에서 구체적으로 주민번호의 처리를 요구하거나 허용한 경우
2. 정보주체 or 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호, 제2호에 준하여 주민번호 처리가 불가피한 경우로서 행정자치부령으로 정하는 경우

발송일
2014. 09

Q

개인정보 이용내역은
연 1회 이상 이메일로
고객에게 통지하고 있습니다

회사DB에는 과거
개인정보수집절차가 없을 때
수집한 개인정보도 있습니다

<개인정보수집동의절차>시행 전 수집한 개인정보도 정보통신망법에 따라 이용내역을 고객에게 통지해야 하나요?

A

X

정보통신망법 제22조, 제23조 1항 단서규정이 없던 때

〈수집동의〉를 거치지 않은 개인정보는 이용내역을 통지할 필요가 없습니다

근거1 정보통신망법 제30조의2에 따른 이용내역통지대상은 제22조, 제23조 1항 단서에 따라 〈수집동의〉를 거친 개인정보임

제30조의2 1항 (개인정보 이용내역의 통지)

정보통신서비스 제공자등으로서 대통령령으로 정하는 기준에 해당하는 자는
제22조 / 제23조제1항 단서에 따라 수집한 이용자 개인정보의 이용내역을 주기적으로 이용자에게 통지하여야 한다

제22조 (개인정보의 수집 · 이용 동의 등)

① 정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다.
다음 각 호의 어느 하나의 사항을 변경하려는 경우에도 또한 같다.
1. 개인정보 수집이용목적 2. 수집정보항목 3. 보유 · 이용 기간

② 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우 제1항에 따른 동의 없이 이용자의 개인정보를 수집 · 이용할 수 있다.
1. 정보통신서비스 제공계약을 이행하기 위해 필요한 개인정보로 경제적 · 기술적 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우
2. 정보통신서비스 요금정산을 위해 필요한 경우
3. 이 법 or 다른 법률에 특별한 규정이 있는 경우

제23조 (개인정보의 수집제한 등)

① 정보통신서비스 제공자는 사상, 신념, 과거의 병력(病歷) 등 개인의 권리 · 이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다.
다만, 제22조 제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 그 개인정보를 수집할 수 있다.

근거2 정보통신망법 및 부칙에 소급적용, 경과조치규정 없음

[참고] 한국정보보호진흥원(현 KISA)발간 TM관련 개인정보보호 설명회(2008) 3p

정보통신망법 중 개인정보보호 조항이 시행된 것은 2000년부터이고 법률은
소급적용되지 않으므로 2000년 이전 가입고객에 대해서는 별도로 동의를 받지 않으셔도 됩니다

참고 정보통신망법 제22조, 제23조 1항 단서에 따라 〈수집동의〉를 거친 개인정보는 이용내역을 통지

O 〈수집동의〉+〈회원가입절차〉없이 수집

O 〈수집동의〉+온라인·방문·전화로 수집

O 〈수집동의〉+국내DB에 저장한 외국인

국적상관없이 개인정보가 국내DB에 있으면
국내법을 적용받음

1	2	3
국내헌법은 외국인의 기본권을 인정	개인정보 자기결정권은 기본권	개인정보=생존하는 개인에 대한 정보 외국인정보도 개인정보에 해당

O 〈수집동의〉+국내DB에 저장한 해외거주한국인

해외거주여부와 상관없이 개인정보가 국내DB에 있으면
국내법을 적용받음

O 〈수집동의〉+ 연락처만 수집한 경우

연락처도 개인정보에 해당
개인정보이용내역 통지방법

핸드폰번호가 있을 경우	집전화번호만 있을경우
SMS, 전화통화	전화통화

방통위 발간 정보통신서비스제공자를 위한 개인정보보호법령 해설서(2012) 102p

참고 정보통신망법 [개인정보 이용내역통지] 란 무엇인가

누가 통지하는가?

정보통신망법 시행령 제17조 1항

정보통신서비스 부문
전년도 매출액 100억원 이상

or

고객 수
100만명 이상

통신 · 민간사업자

누구에게 통지하는가?

정보통신망법 제30조의2

정보통신망법 22조, 23조1항 단서에 따라 개인정보 수집이용에 동의한
정보통신서비스 이용자(=고객)

무엇을 통지하는가?

정보통신망법 시행령 제17조 2항

1
개인정보
수집이용목적/
수집항목

2
제3자제공 관련내용
· 제3자제공업체명
· 제공목적
· 제공된 개인정보항목
* 범죄수사, 법원재판, 국가안보를 위한 통신사실확인 자료제공은 제외

3
취급위탁 관련내용
· 위탁업체명
· 위탁업무내용

언제 통지하는가?

정보통신망법 시행령 제17조 3항

연 1회 이상

어떻게 통지하는가?

방통위, 정보통신서비스 제공자들을 위한 개인정보보호법령해설서(2012), 99~102p

O 가능
이메일, 우편, 팩스, 집전화, 휴대전화,
SMS, 인터넷메시지, 링크연결

X 불가능
(개별통지없이)
웹사이트에 이용내역 게시

발송일
2014. 07

전 제 조 건

본 건은 **금융기관**의 질문을 레터화한 경우로서
주민번호수집에 대한 근거법령에 따라
법적보유기간 내에서 주민번호를 저장하고 있다는 전제 하에 작성되었습니다

Q

주민번호 대신 주민번호와 1:1 대응되는
임의의 서비스 번호를 사용하는 경우

서비스번호는 평문저장 주민번호만 암호화저장이 가능한가요?

A

O

주민번호는
안전한 암호화 알고리즘으로
암호화해야 함

근거

개인정보보호법고시 [개인정보의 안전성 확보조치 기준] 제7조 (개인정보의 암호화)

⑥ 개인정보처리자는
고유식별번호(주민번호,여권번호,운전면허번호,외국인등록번호),비밀번호,바이오정보를
안전한 암호화 알고리즘으로 저장해야한다

⑧ 개인정보처리자는 업무용 컴퓨터에 고유식별정보를 저장하여 관리하는 경우
상용 암호화 소프트웨어 or 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장해야한다

원문보기

2012년 10월 행정자치부 발간
〈개인정보 암호화조치 안내서〉에서 말하는 **안전한 암호알고리즘** (7p)

구분	대칭키 암호 알고리즘 (동일한 키로 암 · 복호화)	공개키 암호 알고리즘 (각자 다른 키로 암 · 복호화)	일방향 암호 알고리즘 (암호화만 가능, 비밀번호에 사용)
알고리즘 명칭	SEED ARIA-128,192,256 AES-128,192,256 Blowfish Camelia-128,192,256 MISTY1 KASUMI 등	RSA KCDSA(전자서명용) RSAES-OAEP RSAES-PKCS1 등	SHA-224,256,384,512 Whirtpool 등

원문보기

발송일
2014. 06

Q DB암호화 시 주민번호 뒷자리만 암호화저장해도 될까요?

A O

구태언 대표변호사님 법률자문 원문보기

근거

행정자치부 [개인정보 위험도분석기준 및 해설서] 2013.03, 13p (암호화의 범위)

원문보기

주민번호는 생년월일과 성별정보를 포함하고 있는
앞 7자리를 제외한 뒷자리 6개번호 이상 암호화하는 것이 바람직하다

평문화	암호화
970325-1	******

수집조건

2014.08.07부터 주민번호 수집법정주의가 실행되었으므로 먼저, 주민번호수집이 법적으로 가능한지 확인해야 함

개인정보보호법 제24조의2 1항 (주민번호처리의 제한)

개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민번호를 처리할 수 없다

1. 법령에서 구체적으로 주민번호의 처리를 요구하거나 허용한 경우
2. 정보주체 or 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민번호 처리가 불가피한 경우로서 안전행정부령으로 정하는 경우

예) 금융기관의 수집가능 VS 수집불가

수집가능 실명거래업무

금융실명거래 비밀보장법률 제32조
금융회사는 거래자 **실지명의**로 금융거래를 하여야한다

금융실명거래 비밀보장법률 제2조
실지명의란 주민등록표,사업자등록증 상의 명의를 말한다

수집불가 홈페이지 회원가입 등 금융거래와 관련없는 업무

행자부 주민번호수집금지제도 가이드라인 14p

홈페이지 회원가입/관리시 주민번호는
생년월일+전화번호조합, 아이핀으로 대체가능하다

참고 주민번호 암호화규정

개인정보보호법 제24조 3항 (고유식별정보의 처리 제한)

개인정보처리자는
고유식별정보가 분실 · 도난 · 유출 · 변조 or 훼손되지 아니하도록
대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다

발송일
2014. 04

전 제 조 건

회사가 건강진단기관(병원)에 건강진단을 의뢰할 때는
법률가에 따라 위탁이라는 견해와 제3자제공이라는 견해가 동시에 존재합니다
본 건은 위탁이라는 전제 하에서 작성되었습니다

Q1

회사는 직원건강검진시 건강진단기관(병원)으로 직원 동의없이 직원 개인정보 (이름, 연락처, 생년월일 등)를 보낼 수 있나요?

A1

위탁이라는 전제하에서

O

Q2 주민번호 관련 질문

Q2-1

회사가 직원 동의를 받으면 직원 주민번호를 병원으로 보낼 수 있나요?

A2-1

X

Q2-2

건강진단을 위해 내원시 건강진단기관(병원)은 직원 주민번호를 직원에게 직접 받을 수 있나요?

A2-2

O

A1의 근거

직원건강검진을 위한 개인정보제공은 개인정보보호법 제26조에 따라 업무위탁에 해당,직원동의없이 보낼 수 있습니다

단, 위탁사실/내용은 직원에게 공개해야 합니다

개인정보보호법 제26조 (업무위탁에 따른 개인정보의 처리 제한)

② 개인정보의 처리 업무를 위탁하는 개인정보처리자(위탁자)는
위탁하는 업무내용과 개인정보 처리업무를 위탁받아 처리하는 자(수탁자)를
정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다

1 회사는 **산업안전보건법 제43조 1항에 따라**
직원의 건강을 보호 · 유지하기 위해 건강진단을 해야 함

산업안전보건법 제43조 1항(건강진단)
사업주는 근로자의 건강을 보호/유지하기 위해
건강검진을 하는 기관에서
근로자에 대한 건강진단을 하여야 한다

2 **직원복지차원의 건강검진**은 **직원만족을 위해 회사가 진행**하는 것
건강검진의 실질적 담당자는 **회사**

3 **업무위탁**일 경우 개인정보유출사고 발생시 **회사 · 병원 모두에게 책임을 물을 수 있음**
즉 직원의 **개인정보 자기결정권**을 더 폭넓게 **보장**할 수 있음

4 **제 3자 제공**일 경우 개인정보를 제공받는 **병원의 이익을 위해 사용**되므로
회사의 예상보다 개인정보를 더 넓게 사용할 가능성이 있음

왜 제 3자 제공이 아닌 업무위탁일까?

업무위탁과 제 3자 제공의 차이점 (서울중앙지법 2011.09.30 선고2008가합49696 판결 참조)

업무위탁	제 3자 제공
정보를 제공하는 측(회사)의 사업목적을 위해 개인정보를 제 3자에게 제공하는 것	**정보를 제공받는 측(병원)의 사업목적을 위해** 개인정보를 제 3자에게 제공하는 것

A2의 근거

개인정보보호법 제24조의2 1항 1호 (주민번호 처리의 제한)

① 개인정보처리자는 다음에 해당하는 경우를 제외하고는 주민번호를 처리할 수 없다
1. 법령에서 구체적으로 주민번호의 처리를 요구하거나 허용한 경우

회사가 건강진단기관(병원)에 직원 주민번호를 제공하는 것이 불가능한 이유

1 개인정보보호법 제16조 1항 〈개인정보최소화의 원칙〉에 위배

회사가 병원에
직원개인정보를 제공하는 목적은
본인임을 확인하여 진단을 원활하게 하기 위함임
▶ 이름, 연락처, 생년월일로도 본인확인가능,
주민번호를 제공할 이유 없음

병원은 검사결과를 기재하는
〈건강진단개인표〉 작성을 위하여
주민번호를 수집할 수 있음
▶ 회사가 건강진단신청단계에서 〈건강진단개인표〉작성을 위하여 주민번호를 대신 수집해서 보내는 것은 개인정보최소수집원칙에 위배됨

2 주민번호 제공을 허용하는 법령이 없음

건강진단기관(병원)이 내원한 직원에게 주민번호를 수집할 수 있는 이유

검사결과를 기재하는 〈건강진단개인표〉 작성을 위하여 법령상 수집허용

노동부고시 [근로자 건강진단 실시기준] 제13조 (건강진단결과의 판정 등)

② 병원이 건강진단을 실시했을 때 그 결과를 별지 6호 서식 건강진단개인표(주민번호포함)에 기록하여 근로자(직원)에게 보내야 한다

발송일
2014. 02

교육기관의 개인정보 이용 OX

안 내

본 질문은 내용의 정확성을 위하여 소만사가 별도의 편집을 하지 않고
고객질문과 변호사의 답변 원문을 그대로 올려드립니다

〈시설물 사용신청서〉(휴대폰번호 사용동의 포함)를 제출한 학생에게 교내 체력단련실에 런닝머신이 들어왔다고 SMS문자를 보내도 될까요?

〈시설물 사용신청서〉 제출시 개인정보 사용 목적을 기재하고, 동의를 받는다면
사용목적 범위 내에서 개인정보를 사용할 수 있습니다.
이 경우 사용 목적 범위 내에 '시설물 구비에 대한 정보전달' 이 명확히 규정되어 있다면 SMS 문자를 보낼 수 있다고 판단됩니다.

학생들에게 편의를 제공하기 위해 〈영상실 사용신청서〉를 받아 처리하고 있는데 이에 대한 동의를 받아야 하나요?

학생들이 대학에서 제공하는 편의시설인 영상실을 사용하기 위하여 〈영상실 사용신청서〉를 제출하는 경우,
위 신청서의 제출만으로 이미 동의 의사를 밝힌 것으로 판단되므로 영상실 사용에 대한 별도의 동의를 받을 필요는 없으나
위 신청서에 개인정보보호법에 따른 고지와 동의를 구현하여야 한다고 판단됩니다.
다만, 영상실 내에 학생들의 활동을 녹화할 수 있는 영상녹화기기 등이 설치된 경우 관련 법령에 따른
적절한 조치를 취할 필요가 있으며 기타 개인정보를 침해할 수 있는 사항이 있는지에 대한
법률 검토가 별도로 필요할 수는 있습니다.

대학내부에서 업무용 교직원·학생 공용주소록(이메일, 휴대폰번호)을 만들어 사용중입니다. 이 때 교직원·학생동의를 받아야 하나요?

개인정보보호법 제15조는 개인정보수집 및 이용시 정보주체로부터 동의받은 목적 범위 내에서 사용하도록 하고 있는 바,
대학 내부의 업무라 함은 그 범위가 구체적이라고 볼 수 없어
어떤 업무를 위해 정보주체의 개인정보를 사용하는지 여부를 명확히 할 필요가 있다고 판단됩니다.
문제는 위 주소록이 외부로 유출되어 제3자에게 제공될 경우
주소록의 수집, 이용, 제공에 대해 법적 책임이 발생될 수 있습니다.
따라서 교직원, 학생의 공용 주소록이 어떤 업무를 위해 사용되는지에 대해 개인정보보호법에 따른
정보주체의 명시적인 고지와 동의가 필요하다고 판단됩니다.

대학교는 교육지원법 제23조 3항에 의해 학생정보를 동의없이 수집할 수 있는데 대학 행정부서 및 학과에서 이 정보를 업무에 활용할 수 있나요?

X

교육기본법 제23조의3

학교생활기록의 정보는 **교육목적으로 수집/처리/이용/관리**되어야 하며,
이에 따른 학생정보는 법률로 정한 경우 외에는 동의 없이 3자에게 제공할 수 없다

위 교육기본법은 초, 중, 고등학교에만 적용되는 것으로서 대학교의 경우 학생정보 수집에 대한 명시적인 규정이 없는 것으로 보입니다. 또한, 위 교육 관련 법률에 규정되지 않은 경우 개인정보보호법이 적용되며, 각급 학교의 경우 행정자치부의 [공공기관의 개인정보보호를 위한 기본지침]에 따라 개인정보 취급방침을 공지하여 학생정보 수집에 대한 동의를 받고 있습니다.
따라서 학생의 명시적인 동의 범위 내에서라면 행정부서 및 학과에서는 학생정보를 업무에 활용할 수 있을 것으로 판단됩니다.

대학교 졸업사진 촬영 후 졸업앨범에 학생의 동의를 받고 성명·사진을 게시해야 하나요?

X

행정자치부 '개인정보 보호법령 및 지침고시' 72p (2011.12)

개인정보처리자는 정보주체의 동의를 받은 경우 개인정보를 수집할 수 있는데, '동의'는 개인정보처리자가 개인정보를 수집/이용하는 것에 대한 정보주체의 자발적인 승낙의 의사표시로서(서명날인, 구두, 홈페이지 동의 등) 동의여부를 명확하게 확인할 수 있어야 한다

대학교 졸업앨범의 경우 각 학교별로 선택사항으로 운영하고 있어 졸업 앨범 촬영을 원하는 학생들만 이에 응하고 있습니다. 그렇다면 촬영에 응한 학생은 자발적으로 자신의 성명 및 사진의 게시에 대해 동의한 것으로 볼 수 있으므로 사진 촬영행위 그 자체로서 동의 여부를 확인할 수 있는 것으로 판단됩니다.
따라서 학생에 대해 별도 서면동의 등 명시적 동의를 받을 필요는 없다고 생각됩니다.

교직원 A의 개인 업적증빙자료에 타인인 B의 개인정보가 포함되어 있다면 교육부에 공문으로 보낼 수 있나요?

X

행정자치부 '개인정보 보호법령 및 지침고시' 72p (2011.12)

개인정보의 처리란 개인정보의 수집/생성/기록/저장/보유/가공/편집/검색/출력/정정/복구/이용/제공/공개/파기/ 그 밖에 이와 유사한 행위를 말한다.
'그밖에 이와 유사한 모든 행위'에는 개인정보의 전송/전달/열람/이전/공유/위탁 등이 포함될 수 있다.

교직원 A의 업적증빙자료를 공공기관인 교육부에 보내는 행위는 교직원 A뿐만 아니라 타인인 B의 개인정보를 제3자에게 송부하는 행위이기 때문에 개인정보의 처리 행위에 포함된다고 볼 수 있습니다.
따라서 이에 대해 정보주체인 타인 B의 명시적인 동의를 받거나, 아니면 이러한 개인정보의 수집, 이용, 제공에 대해 법령의 특별한 규정이 필요하다고 판단됩니다.
만약 이에 대해 B의 동의를 받을 수 없거나 법령의 특별한 규정이 없는 경우 B의 개인정보를 마스킹처리하거나 삭제하는 등 적절한 조치를 취함으로써 제3자에게 B의 개인정보가 도달하지 않도록 하여야 합니다.

발송일
2014. 02

Q 수탁업체점검시 반드시 전수점검 해야 하나요?

A O

Q 수탁업체 개인정보취급자 전원에게 개인정보교육을 해야하나요?

A O

근거

개인정보보호법 제26조 (업무위탁에 따른 개인정보의 처리 제한)

④ 위탁자는 개인정보가 분실·도난·유출·변조 · 훼손되지 않도록 수탁자교육, 처리현황점검 등 수탁자가 개인정보를 안전하게 처리하는지 감독해야 한다

⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당업무범위를 초과하여 개인정보를 이용하거나 제3자에게 제공해서는 안된다

⑥ 수탁자가 위탁받은 업무관련 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속직원으로 본다

부분점검,
개인정보취급자 일부 대상 교육은
수탁자에 대해 상당한 주의를 기울여
관리 감독한것으로 볼 수 없음

수탁자가 개인정보유출사고를
일으키면 위탁자도 책임져야함

행자부 '개인정보 보호법령 및 지침고시 해설서'
: 개인정보취급자에 대한 정기적 교육, 199p (2011.12)

연간 교육계획을 수립하여 모든 개인정보취급자가
일정시간 이상 교육에 참여하도록 해야 한다

모든 개인정보취급자에게
교육해야한다고 명시되어있음

27p [개인정보의 안전성 확보조치 기준] 규정 보기

위탁자는 수탁자가
개인정보보호법고시 [개인정보의 안전성 확보조치 기준]을 준수하는지 점검해야함

발송일
2014. 02

Q1 사망자정보는 개인정보 인가요?

A1 X

Q2 (상호명, 사업자번호 등) 법인,단체정보는 개인정보 인가요?

A2 X

A1의 근거

개인정보보호법 제2조 1항 (정의)

살아있는 개인에 관한 정보로서 성명, 주민번호, 영상 등을 결합하여 개인을 알아볼 수 있는 정보

행정자치부 '개인정보 보호법령 및 지침고시 해설서' 7p (2011.12) 원문보기

개인정보 보호법익인 프라이버시권(사생활의 비밀과 자유)은 인격권에 해당한다.
인격권은 자신의 인격보호를 위한 권리이므로 상속이 불가능하다.
사망자는 자신의 정보에 대한 권리를 행사, 상속할 수 없으므로 사망자의 정보는 개인정보로 볼 수 없다.

→ 다만,
사망자의 정보가 사망자와 유족과의 관계를 나타내는 정보이거나 유족, 지인의 사생활을 침해할 경우 사망자 정보인 동시에 유족 정보이기도 하므로 **개인정보보호법에 따른 보호대상이 될 수 있음**

A2의 근거

행정자치부 '개인정보 보호법령 및 지침고시 해설서' 7p (2011.12) 원문보기

개인정보의 주체는 현재 생존하고 있는 자연인을 의미한다.
따라서 법인이나 단체에 관한 정보는 원칙적으로 개인정보에 해당하지 않는다.

→ 따라서,
법인 or 단체의 이름(상호), 사업자등록번호, 영업소
주소, 전화번호, 대표자 성명 등 임원 현황, 자산 or 자본 규모, 주가,
영업실적, 납세실적, 영업비밀 등은 개인정보보호법에 따른 보호대상이 아님
* 다만 기업의 영업비밀은 '부정경쟁방지 및 영업비밀보호에 관한 법률'에 의하여 보호를 받음

발송일
2014. 02

Q 고객은 회사에게 자신의 개인정보처리내역에 대하여 열람요구를 할 수 있나요?

A O

전제조건
고객은 〈개인정보 열람요구서〉를 제출해야 함

〈개인정보 열람요구서〉

▪ 개인정보보호법 시행규칙 [별지 제8호서식]

개인정보([✓] 열람 [ ]정정 삭제 [ ]처리정지) 요구서

요구항목 표시

아래 작성방법을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.

접수번호	접수일	처리기간 10일이내
		신청서 받은 날로부터 10일이내로 처리해야함
정보주체	성 명	전화번호
	생년월일	
	주소	
대리인	성 명	전화번호
	생년월일	정보주체와의 관계
	주소	
요구내용	[✓] 열람 요구사항을 표시하여 개인정보처리자에게 제출	[✓] 개인정보의 항목/내용
		[✓] 개인정보 수집/이용의 목적
		[✓] 개인정보 보유/이용 기간
		[✓] 개인정보의 제3자 제공 현황
		[✓] 개인정보 처리에 동의한 사실/내용
	[ ] 정정/삭제	* 정정/삭제하려는 개인정보의 항목과 그 사유를 적습니다.
	[ ] 처리정지	* 개인정보의 처리정지를 원하는 대상, 내용 및 그 사유를 적습니다.
[개인정보 보호법] 제35조제1항 · 제2항, 제36조제1항 or 제37조제1항과 같은 법 시행령 제41조제1항, 제43조제1항 or 제44조제1항에 따라 위와 같이 요구합니다.		
		년 월 일
	요구인	(서명 or 인)
OOOO	귀하	

근거

고객=정보주체, **회사**=개인정보처리자

개인정보보호법 제35조 1항 (개인정보의 열람)

정보주체는 개인정보처리자가 처리하는
자신의 개인정보에 대한 열람을
해당 개인정보처리자에게 **요구 할 수 있다**

개인정보보호법 시행령 제41조 1항 (개인정보의 열람절차 등)

정보주체는 자신의 개인정보에 대한 열람을 요구할 때
열람사항을 표시한 개인정보 열람요구서를
개인정보처리자에게 제출해야 한다

회사는 고객의 열람요구사항 중 열람을 거절/제한해야하는 항목을 확인해야 함

개인정보보호법 제35조 4항 (개인정보의 열람)

개인정보처리자(회사)는 다음의 경우, 정보주체(고객)에게 사유를 알리고 열람을 제한/거절할 수 있다

1. 법률에 따라 조회 금지/제한되는 경우

2. 타인의 생명/신체를 해하거나 재산/이익을 침해할 수 있는 경우

3. 공공기관이 다음 항목에 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우

- 조세 부과/징수, 환급관련 업무
- 학교, 평생교육시설, 전문대, 대학, 대학원에서의 성적평가, 입학자선발관련 업무
- 학력/기능/채용시험, 자격심사관련 업무
- 보상금/급부금 산정관련 업무
  국가나 공공 단체에서 내어 주는 돈
- 다른 법률에 따라 진행중인 감사/조사관련 업무

고객이 열람요구할 수 있는 개인정보 범위

회원가입시 정보주체가 직접 제공한 개인정보	개인정보처리자가 제3자로부터 수집한 개인정보	개인정보처리자가 생산한 개인정보	서비스 제공과정 중 생성된 개인정보
이름, 주소, 생년월일, 성별, 연락처, 계좌, 주민번호 등	마케팅대행사, 리서치기관 등	구매성향, 시청률, 신용도, 평균연령, VIP고객선별 등	수발신내역, 입출기록, 쿠키, 로그 등

발송일
2013. 12

안 내

소만사가 테크앤로 법률사무소에 의뢰하여 작성한
SAP어플리케이션 관련 법률자문서입니다
읽으시는 분의 이해를 위하여 OX법률자문 형태의 요약과 변호사 원문을 같이 실었습니다

Q SAP어플리케이션은 개인정보보호법, 정보통신망법 상 <개인정보처리시스템>인가요?

A O

결론

〈개인정보처리시스템〉에 연계 연동된 **SAP어플리케이션**은 행정자치부, 방송통신위원회 및 사법기관에 의하여 〈개인정보처리시스템〉으로 판단될 가능성이 매우 높아졌다

상대적으로 안전조치가 취약한 **SAP어플리케이션**을 통해 개인정보의 침해가능성이 높아질 것으로 예상되므로 앞으로 행정기관, 사법기관에서 **개인정보의 안전성 확보조치가 SAP어플리케이션** 보호까지 확대되어야 하는 것으로 판단할 가능성이 매우 높아졌다

근거

공공기관의 개인정보 영향평가 대상은 DB시스템 or **어플리케이션** 프로그램 등의 〈개인정보처리시스템〉 이다

(행자부, 공공기관 개인정보영향평가 수행안내서(개정판), 12면)

〈개인정보처리시스템〉에 **어플리케이션** 등도 포함시키는 것이 타당하다

(방통위, 정보통신서비스 제공자등을 위한 외부인터넷망 차단조치 안내서. 1-3. 용어의 정의)

개인정보 유출방지를 위해 적용하는 망분리 정책은 **어플리케이션**에 적용된다

(방통위, 정보통신서비스 제공자등을 위한 외부인터넷망 차단조치 안내서, 2면)

[법률자문서 원문]

TEK&LAW

서울 종로구 종로 1 교보빌딩 15층 테크앤로 법률사무소 T: (02)2010-8840 F: (02)2010-8985

수 신 : 주식회사 소만사

참 조 :

발 신 : 테크앤로 법률사무소 변호사 구태언

일 자 : 2013. 8. 1.

제 목 : SAP 어플리케이션이 〈개인정보처리시스템〉 인지 여부

위 제목의 건에 대하여 아래와 같이 본 법률사무소의 의견을 드리오니 업무에 참고하시기 바랍니다.

1. 질의의 요지

귀사는 ERP 인 SAP (이하 'SAP'이라 합니다.)에 대한 개인정보보호 솔루션인 APP-i 를 판매하면서 SAP 도 개인정보 보호법상 〈개인정보처리시스템〉에 포함되는지를 문의하셨습니다.

2. 적용 법조

SAP 이 다루는 데이터베이스(DB)에 어떠한 개인정보가 들어 있느냐에 따라

아래와 같이 개인정보 보호법과 정보통신망법의 적용이 달라집니다.

✔ SAP DB 에 협력업체, 내부임직원 정보가 들어 있는 경우

- 개인정보보호법 적용 대상

✔ SAP DB 에 정보통신서비스 이용자로서 고객 DB 가 들어 있는 경우(영리목적 온라인서비스 고객 DB)

- 정보통신망법 적용 대상

✔ SAP DB 에 정보통신서비스 이용자가 아닌 고객 DB 가 들어 있는 경우
(비영리목적 온라인서비스 고객 DB or 오프라인서비스 고객 DB)

- 개인정보보호법 적용 대상

3. 문헌조사

가. 관련규정

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

제15조 (개인정보의 보호조치)

② 법 제28조제1항 제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 다음 각 호의 조치를 하여야 한다.

〈단서 생략〉

1. **개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 "〈개인정보처리시스템〉"이라 한다)**에 대한 접근권한의 부여 · 변경 · 말소 등에 관한 기준의 수립 · 시행 〈각호 생략〉

개인정보의 안전성 확보조치 기준

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

9. "**〈개인정보처리시스템〉"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템**을 말한다. 다만 소상공인 or 중소사업자가 내부 직원의 개인정보만을 보유한 시스템은 제외한다.

표준 개인정보 보호지침

제2조(용어의 정의) 이 지침에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보 처리"란 개인정보를 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
7. "**〈개인정보처리시스템〉"이란 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템**을 말한다.

개인정보의 기술적 · 관리적 보호조치 기준

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

4. "**〈개인정보처리시스템〉"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.**
5. "망분리"라 함은 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단하기 위해 업무망과 외부 인터넷망을 분리하는 망차단조치를 말한다.

나. 관련 감독기관의 해설서 등 공간된 문헌

개인정보의 안전성 확보조치 기준 및 해설서

9. "〈개인정보처리시스템〉"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다. 다만 소상공인 or 중소사업자가 내부 직원의 개인정보만을 보유한 시스템은 제외한다.
   - "〈개인정보처리시스템〉"이란 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.
   - 〈개인정보처리시스템〉은 일반적으로 개인정보의 체계적인 처리를 위한 DBMS (Database Management System)을 말한다.

정보통신서비스 제공자등을 위한 외부 인터넷망 차단조치 안내서(2013. 2.)

1-3 용어의 정의

"〈개인정보처리시스템〉"이란 개인정보를 이용한 데이터 처리를 위해 체계적으로 구성한 데이터베이스 관리시스템(DBMS)을 말하며, **개인정보 DB에 접근하기 위한 중계서버, 어플리케이션 등도 포함시키는 것이 타당하다.**

4. 〈개인정보처리시스템〉의 개념

가. 쟁점의 정리

SAP이 〈개인정보처리시스템〉에 해당하는지 여부를 검토하기 위해서는
〈개인정보처리시스템〉의 개념이 먼저 확정되어야 할 것입니다.

이를 위해 관련 법령상에 규정되어 있는 〈개인정보처리시스템〉의 정의에 대해 살펴본 후,
〈개인정보처리시스템〉에 대한 다양한 견해를 검토하여 〈개인정보처리시스템〉에 대한 개념을 설정하고자 합니다.

만약 SAP 이 〈개인정보처리시스템〉에 해당된다면, 개인정보처리자는 SAP 에 대해 ① 접근 권한의 관리 의무 ② 접근 통제 시스템 설치운영 의무 ③ 접속기록의 보관 및 위·변조 방지 의무 등을 부담할 것입니다. (개인정보의 안전성 확보조치 기준)

나. 〈개인정보처리시스템〉의 정의

개인정보의 안정성 확보조치 기준 제2조 제9호 등에 의하면 〈개인정보처리시스템〉이라 함은 **개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템**을 말합니다.

그러나 '데이터베이스시스템'이라는 용어가 포함하는 범위가 모호한 면이 있어 아래와 같이 의견이 대립되고 있습니다.

다. 〈개인정보처리시스템〉은 DBMS 로 한정하여야 한다는 견해

〈개인정보처리시스템〉은 개인정보 처리의 해석 등을 이유로 DBMS 로 한정하여야 한다는 견해가 있으며,
구체적인 근거는 다음과 같습니다.

- 〈개인정보처리시스템〉에 접속하는 어플리케이션과 개인정보 중계서버는 다른 사람이 처리하고 있는 개인정보를 단순히 전달, 전송 or 통과만 시켜주는 행위로서 개인정보의 처리에 해당하지 아니하는 점[1]
- 해커가 온라인으로부터 접수되는 상담을 효율적으로 처리하기 위한 어플리케이션 서버에 침입하는 것이 곧바로 데이터베이스 서버에 대한 침입으로 연결되지 아니하는 점[2]

라. 〈개인정보처리시스템〉에 어플리케이션, 중계서버가 포함된다는 견해

〈개인정보처리시스템〉에 접근하기 위한 어플리케이션, 중계서버는 개인 정보를 사실상 처리하고 있어
〈개인정보처리시스템〉에 해당한다는 견해이며, 구체적인 근거는 다음과 같습니다.

- 〈개인정보처리시스템〉이란 개인정보를 이용한 데이터처리를 위해 체계적으로 구성한 데이터베이스 관리시스템(DBMS)을 말하며, 개인정보 DB 에 접근하기 위한 중계서버, 어플리케이션 등도 포함시키는 것이 타당하다는 점[3]
- 공공기관 개인정보영향평가 가이드에 의하면 〈개인정보처리시스템〉을 신규로 구축하는 경우 '기존 개인정보파일을 관리하던 데이터베이스 시스템 or 어플리케이션 프로그램 등의 〈개인정보처리시스템〉이 노후하여 이를 신규로 구축하고자 하는 경우'라 기술되어 있는데, 이는 어플리케이션 등의 데이터베이스 시스템이 아닌 프로그램도 〈개인정보처리시스템〉이 될 수 있다는 것을 전제로 한 표현인 점[4]

1 행정자치부, 개인정보 보호법령 및 지침고시 해설서, 10면
2 서울중앙지방법원 2010. 1. 14. 선고 2008가합31411 판결 참조
3 방송통신위원회, 정보통신서비스 제공자등을 위한 외부 인터넷망 차단조치 안내서, 2면
4 안정행정부, 공공기관 개인정보 영향평가 수행 안내서(개정판), 12면

- 개정 정보통신망법에서 〈개인정보처리시스템〉에 접근하는 컴퓨터 등의 망분리 조항이 신설된 것은 개인정보 유출 위험성이 있는 개인정보취급자의 컴퓨터 등에 대해 외부망을 차단하는 방법으로 업무망이 아닌 곳에서는 개인정보의 처리를 할 수 없도록 한 것인 점[5]
- 방송통신위원회 개인정보보호포탈 FAQ 에서 개인정보의 조회 · 저장 · 관리를 위하여 데이터베이스가 아닌 파일처리시스템 등으로 구성한 경우라도 개인정보를 처리하고 있기 때문에 〈개인정보처리시스템〉으로 보아야 한다고 기술하고 있는 점[6]

5. 결론

살피건대 아래와 같은 이유로 〈개인정보처리시스템〉에 접근하기 위한 어플리케이션, 중계서버도 행정자치부, 방송통신위원회, 사법기관에 의해 **〈개인정보처리시스템〉으로 판단될 가능성이 매우 높아졌다고** 사료됩니다.

- 어플리케이션은 사용자의 명령에 따라서 DB 에 저장된 데이터를 변경 · 삭제 · 추가하는 역할을 수행하므로 이는 개인정보보호법상의 처리에 해당할 가능성이 높고, 또한 어플리케이션 자체에서 이용하는 고객관련 자료, 임직원의 주민번호, 계좌번호, 이름, 연락처 등과 같은 개인정보 DB 나 개인정보파일을 조회 · 저장 · 관리하는 것 역시 개인정보 처리에 해당하는 점
- 상대적으로 안전조치가 취약한 어플리케이션이나 중계서버를 통해 개인정보의 침해가능성이 높아질 것으로 예상되므로, 앞으로 행정기관, 사법기관에서 개인정보의 안전성 확보조치가 애플리케이션 보호까지 확대되어야 하는 것으로 판단할 가능성이 매우 높아진 점
- 개인정보 DB 가 어플리케이션서버에 저장되어 있지 아니하고 네트웍으로 연결되어있다 하여도, DBMS 시스템에 접속하는 방식은 DBMS 의 서비스 포트에 연결하는 방식으로서 〈개인정보처리시스템〉과 동일하다는 점
- 개인정보 DB 가 아닌 개인정보 파일이 저장되어 있다고 하여도 어플리케이션 입장에서는 OS 에서 제공되는 파일 입출력 API 를 사용하거나 DB Connection API 를 사용한다는 점에서 차이가 있을 뿐 개인정보의 열람 · 수정은 동일한 방식으로 제공된다는 점
- 방송통신위원회가 '정보통신서비스 제공자등을 위한 외부 인터넷망 차단조치 안내서'(2013. 2.)에서 같은 견해를 취하고 있는 점

따라서 개인정보보호법의 입법 취지, 개인정보보호 필요의 당위성 등을 종합하여 볼 때 행정기관, 사법기관에서 사실상의 개인정보 처리가 수행되고 있는 어플리케이션, 중계서버에 대해서도 위 관련부처, 사법부에 의해 개인정보 처리시스템이라고 판단할 가능성이 매우 높아진 상황으로 보입니다.

다만 위에서 언급하였듯이 위 견해를 취한다고 할지라도 일률적으로 어플리케이션 서버인 SAP 서버가 〈개인정보처리시스템〉에 해당한다고 판단할 것이 아니라, **SAP DB 에 개인정보가 들어있으면 개인정보를 처리하는 것이므로 개인정보 처리시스템이 될 것이고, 개인정보를 조회 or 수정하지 않는다면 개인정보 처리시스템에 해당하지 않는다고 보아야 할 것**입니다.

이상과 같이 의견을 드리오니 업무에 참조하시기 바랍니다.

TEK&LAW

5 방송통신위원회, 정보통신서비스 제공자등을 위한 외부인터넷망 차단조치 안내서, 2면
6 개인정보보호 포털, 자주하는 개인정보 질문,
http://www.jprivacy.kr/servlet/command.user.notice.FAQRead?faqidx=162&currentPage=9&select_condition=&select_option1=0

소만사의 마음에 영원히 남을
UnSung Hero의 편지

"소"잃고 외양간 고치지 말고 "만"일의 사태에 대비하는 보안업무야말로 "사"랑하고도 사랑하는 IT의 근본이다. 이를 17년 동안이나 묵묵히 지켜주시는 "소만사" 진심으로 축하를 드립니다. 계속 주식으로써의 보안업무를 지켜주세요. 〈공공○○님〉 2011년 소만사의 개인정보교육을 처음 듣고서 소만사에 대해 알았습니다. 그리고 그 계기로 CPPG를 취득하여 업무에 큰 도움을 받고 있고 계속적인 소만사의 정보로 업무에 적용할 수 있어서 감사드립니다. 소만사가 17년의 긴 역사인 것은 몰랐습니다. 저희 나라에도 이렇게 오래 전부터 정보보호 일익을 담당하는 회사가 있었구나 하니 요즘처럼 어지러운 시국에 든든한 마음입니다. 소만사 창립 17주년 축하드리며 앞으로 20년 50년 쭉~ 정보보호의 주식으로 자리 매김하여 주시길 부탁드리겠습니다. 〈기업 ○○님〉 10년이상 소만사와 한솥밥을 먹은 것 같습니다. 앞으로 계속 좋은 솔루션으로 좋은 기업으로 대한민국의 IT를 선도하는 1등 기업으로 발전하시길 바랍니다. 진심으로 축하합니다. 〈A기술 ○○님〉 14년전에 웹키퍼로 처음 인연을 맺었는데 이제 17년차가 되셨다하니 진심으로 축하드립니다. 앞으로도 계속 번창하셔서 대한민국 일등 보안업체가 되시길 기원할께요. 〈공공 ○○님〉 17×365=6205 번의 해가 뜨고 졌네요. 다음 6205번도 기대하겠습니다. 〈기업 ○○님〉 17년 되신것 많이 많이 축하드려요 71년 될때까지 계속 1등하시고 무궁한 발전이 있기를 바랍니다. 그런 의미에서 삼행시... 소: 소만사 17년 축하드려요. 만: 만족할 만한 솔루션 항상 만들어주시고 사: 사은품으로 쌀까지 주시니 소만사는 센스쟁이!!! 〈기업 ○○님〉 말 긴 17년 정안이라 시간 보운 시장에서 살아남으시고 보안의 큰 축으로 역할을 담당하고 있는 것을 정말 축하합니다. 앞으로도 전세계 보안시장의 메인으로 거듭나시길 바랍니다. 앞으로도 100주년 200주년 계속 이어갈수 있길 바랍니다. 〈기업 ○○님〉 17년... 사춘기를 잘 마치고 이제 안정적인 미래를 꿈꾸는 시기로 접어드는 해인것 같습니다. 트래픽 속에 숨어 있는 다양한 보호이슈들이 소만사와 함께 더욱 가치있게 보호되기 기대해 봅니다. 앞으로는 "소중하게 만족시켜 가는 사람들" 〈공공○○님〉 17년~!!! 정말 어려운 시간들을 잘 이겨내고 큰 기업으로 성장하셨네요. 창립기념을 축하드립니다. 이제 글로벌 기업으로 또 다시 한단계 업그레이드되기를 기원합니다. 소만사~!! 파이팅~!! 〈기업 ○○님〉 17년이란 세월동안 일관된 영역에서 한결같은 서비스를 제공해온 '소만사' 특이한 이름으로 저에게 첫인상을 남긴지도 10여년이군요. 창립 17주년 진심으로 축하드리며 앞으로도 쭉~ 한결같은 서비스 기대합니다. 가끔씩 진행하는 이색적인 이벤트도 재밌게 보고있습니다. 〈단체○○님〉 17년째로 접어들으셨다구요...진심으로 축하드립니다. 열악한 보안시장에서 꿋꿋이 자리매김하셔서 당당히 한 영역을 구축하셨다는 생각이 듭니다. 앞으로도 더욱 노력하셔서 대한민국의 보안회사로서의 브랜드가치를 더욱 높이시기를 진심으로 기원드립니다. 감사합니다. 〈은행 ○○님〉 1997년 IMF 어려운 시대에 태어나 힘든 격정의 시기를 넘어 현재는 국산 소프트웨어의 중심에 서있는 소만사. 나날이 증가되는 보안화두에 발맞추어 앞서나가고 있는 기업으로서 앞으로도 무궁무진한 발전과 희망이 있기를 바랍니다. 17주년 축하드립니다. 〈공공 ○○님〉 개인정보보호법의 시행으로 개인정보보호의 중요성이 강조되고 사회적 인식도 많이 변화되었습니다. 이와 관련하여 귀사가 개인정보보호에 오랜 동안 기여함에 감사드리고 창립 17년을 축하드리며 앞으로도 국가 정보화 및 개인정보보호에 더욱 힘써 주시기를 기대하겠습니다. 다시 한번 더 귀사의 건승을 기원합니다. 〈공공 ○○님〉 고객과의 소중한 만남을 사랑하는 소만사. 고객의 소중한 정보를 만족스럽게 지켜주는 소외되지 않는 사회적인 기업으로 번창하심을 기원하겠습니다! 다시 한번 창립 17년을 축하드립니다. 〈기업 ○○님〉 소: 소만사 한솥밥 식구 여러분 모두 만: 만사형통하는 계사년 보내시길 진심으로 기원합니다. 사: 사알짝 식상하긴 하지만 제가 보안업무를 시작한지 얼마 안되어 새해인사도 못 드린것 같아 1분기가 지난 지금에서야 인사드립니다. 앞으로도 더욱 번창하셔서 세계속으로 뻗어나가시길 기원합니다. ^3^~〈기업○○님〉 소 : 소프트웨어장인들이 모여 땀흘리는 회사 만 : 만사형통하시고 사 : 사업이 나날이 번창하시길 기원합니다. 〈기업○○님〉 소 : 소만사는 보안전문회사입니다. 다른 보안전문회사들도 많지만 그 중 단연 최고입니다. 사: 사랑합니다. 그리고 창립 17주년 축하드립니다. 짝짝짝~ 〈기업 ○○님〉 소: 소만사 여러분 만: (많)은 사람들에게 앞으로도 많이 많이 사: 사랑 받으실 거예요.. 〈은행 ○○님〉 소: 소리없는 곳에서 일하는 우리들의 만: 만능 똑똑이 소만사 솔루션 사: 사랑해요~ 〈기업 ○○님〉 소만사는 보안이라는 경직되고 무섭고 딱딱하다고 할 수 있는 분야에서 참 기계적이지 않은 스토리가 있는 곳임이 느껴집니다. 창립 17주년 축하하고 앞으로 170년 1700년 쭉 이어 가시길 바랍니다. 〈연합회 ○○님〉 보안이란 부분이 "별식"이 아니라 "주식"이란 표현에 대해 너무도 공감이 갑니다. 소만사 17년차를 맞이하여 국내뿐 아니라 글로벌기업으로 맛있는 주식으로 자리매김을 할 수 있도록 건승을 빕니다. 축하드립니다. 〈기업 ○○님〉 벌써 보안에서 17년이 되었군요. 보안하면 먼저 소만사 제품이 생각납니다. 앞으로 정보보안

2년 전 창립기념일
보안담당자분 2만여분께
소만사 17년차를 축하해주십사
편지로 부탁드렸습니다

그리고 쏟아졌던 끝없는 답장들
눈물로 감동으로 지새며 읽었던
보안담당자분들의 마음이었습니다

및 개인정보보호부분에서 더 활약 기대하며 좋은 제품 많이 제공해주세요~ 축하드립니다. - 보안으로 17년이지만 100년을 넘어 굳건하게!! - 〈연구원 ○○님〉 벌써 그렇게 되었나요? 이제 질풍노도의 사춘기에 접어들었네요. 열정과 젊음이 있는 한 꿈꾸는 목표를 이룰 수 있을 것으로 확신합니다. 그래서 17년 사춘기를 격하게 축하드립니다. 〈공공 ○○님〉 벌써 17년이라.보안이 점점 중요해지고 말도 많고 탈도 많았는데 그동안 항상 변치않는 서비스와 품질로 고객들의 의견을 들어주시는 소만사가 있어서 든든하네요^^ 앞으로 17년이 아니라 170년동안 건승하시는 기업으로 남기를 바라겠습니다. 아..항상 좋은 서비스 감사합니다.^^ 〈기업 ○○님〉 몸에 좋은 17차...~ 보안에 좋은 17년차 소만사...~!!! 창립 17년을 축하하며 앞으로도 쭈~욱 건승하여 담번엔 27년차 축하메세지를 전하고 싶습니다. 소만사 화이팅~! 〈증권 ○○님〉 그동안 귀사와 더불어 동고동락한게 엊그제 같은데 벌써 17년이라는 세월이 흘렀네요. 향후에도 동반성장의 밑거름이 되어주는 멋진 소만사가 되시길 기원합니다. 축하드립니다~ 〈기업 ○○님〉 국내 대표적 보안소프트웨어 개인정보보호전문기업 소만사의 창립 17년을 진심으로 축하드립니다. 앞으로도 국내 소프트웨어기술 향상을 위해 더욱 노력해주시길 바랍니다. 앞으로 세계적인 소프트웨어기업으로 성장하시길 기원합니다. 감사합니다! "비상하는 한국경제 다시 뛰는 SW" 〈협회 ○○님〉 소: 소신있게 지켜온 보안회사 만: 만사 제쳐놓고 보안을 지켜온 회사 사: 사랑받는 회사. 소만사 소만사 17년을 진심으로 축하합니다. 〈기업 ○○님〉 소만사 개인정보보보호에 있어서는 정말 최고의 기업입니다. 이름도 잘만드셨고 고객관리도 그렇고..매번 받아보는 프라이버시레터 너무 도움됩니다. 앞으로도 무한발전하시길 기원합니다. 〈공공 ○○님〉 소만사 창립 17년을 진심으로 축하드립니다. 전직장에서 제가 소만사 Mail-i를 2002년에 접하게 되었습니다. 저두 벌써 10년이 훌쩍 넘었네요. 다시한번 축하드리며 귀사의 무궁한 발전을 기원합니다. 감사합니다. 〈기업 ○○님〉 소만사 창립 17년차 축하드립니다. 요즘 IT환경이 어려운 가운데 국내기술력으로 보안업계 1위를 하고 있는 소만사를 보며 IT업계의 일원으로써 자부심을 느낍니다. 앞으로도 나날이 번창하시고 승승장구하시길 기원합니다. 〈제약 ○○님〉 소만사 창립 17주년 진심으로 축하 드립니다. 더욱 보안역사에서 빛나는 역할 부탁드립니다. 소: 소프트웨어만 만드는 회사 아닙니다. 만: 만나보면 좋은친구같은 회사 입니다. 사: 사회에서 꼭 100년 가야 할 기업이란 것을〈위원회 ○○님〉 소만사 창립17주년 축하드립니다~ 더욱 번창하세요~ 축하기념으로 삼행시 소: 소중한 사람들과 만: 만남을 이어가 창립 17주년을 맞이했습니다. 사: 사람들과의 만남을 지속적으로 이어가 번창하세요~~^-^ 〈기업 ○○님〉 소만사 창립17주년을 진심으로 축하드립니다. 사내 정보보안 및 중요정보 유출차단을 위해 소만사에서 지원해주신 다양한 정보와 솔루션을 통해 큰 사고없이 하루하루를 보내고 있습니다. 앞으로도 지속적인 관심과 지원을 부탁드리며 더 좋은 솔루션과 보안정책으로 보안사고를 최소화할 수 있는 기준을 제시하는 좋은 파트너가 되었으면 합니다. 귀사의 무궁한 발전을 기원합니다. 감사합니다. 〈기업 ○○님〉 소만사 창립 17주년을 진심으로 축하드립니다. 지난해 롯데호텔서 소만사에서 협찬했던 개인정보보호 관련 쎄미나에서 처음으로 "소중한 만남을 사랑하는"의미의 회사명을 접하고 처음 뵙게된 대표이사님 얼굴이 참으로 회사명과 많이 닮았다는 느낌을 받았었지요! 물론 직원분들도 너무 친절해서 좋았습니다. 그때 받았던 첫 인상! 아직도 생생합니다. 다시한번 진심으로 축하드리고 소만사의 무한한 성장과 안정 모두 이루시기를 간절히 기원합니다!... 감사합니다. 〈건설 ○○님〉 소만사 창립 17주년을 진심으로 축하드립니다. 그동안 여러모로 소만사 소속직원 분들로부터 도움을 많이 받아 항상 감사하게 생각하고 있습니다. 제품이 아무리 뛰어나도 직원 분들이 친절하지 않으면 그 제품을 구입하고 싶지 않더라구요. 그런데 소만사 제품은 뛰어나기도 하지만 직원 분들도 아주 친절하시더라구요. 그 점에서 깊은 감동을 받았습니다. 워낙 여러 업체를 상대하다보니 실력이 있는지 없는지 친절한지 안한지.. 가리게 되더라구요...앞으로도 귀사의 발전을 빌겠습니다!! 〈공공 ○○님〉 소만사 창립 17주년을 축하드립니다. 귀사의 무궁한 발전을 기원합니다. 우리 나라 IT보안의 나아갈 길을 밝히는 또 하나의 꿋꿋한 등대가 되어 주시길 기원합니다. 〈증권 ○○님〉 소만사 창립 17주년을 축하드립니다. 저희 회사에서는 소만사의 개인정보보호시스템과 DB감사시스템을 도입하여 사용중인데요 납품 이후에도 꾸준히 유지관리를 해주시는 덕분에 해당 시스템의 효용성과 효과성이 높아지고 있습니다. 앞으로도 성능과 기능 모두 보장되는 훌륭한 솔루션 개발이 이어지시길 바라며 지속적인 교류가 함께 했으면 좋겠습니다. 다시 한번 창립을 축하드립니다. 〈증권 ○○님〉 소만사 창립을 진심으로 축하드립니다. 소만사의 신뢰성 있는 보안제품들에 관심이 많습니다. 세미나에서 자주 접하고 가능하면 방문하시고 만나뵙는 기회가 앞으로 더욱더 많았으면 좋겠습니다. 다시 한번 축하드립니다!! 〈기업 ○○님〉 안녕하세요~ 사회에 첫 발을 내딛을 때부터 소만사를 안지도 5년이 넘었네요. 참 친숙하지용~ㅎ 소만사 직원분들이 친절하게 도와주셔서 이자리를 빌어 너무 감사드립니다. 이젠 가족 같기도 해요~^__^ 내실이 튼튼하면서도 보안업계 100년이 넘는 기업되기를 바라겠습니다. 그리고 지속적으로 쭉 같이 함께 했으면 좋겠습니다. 소만사 창립 17년차 진심으로 축하드립니다. 〈기업 ○○님〉 십년이면 강산도 변한다는데 한분야를 무려 17년 동안이나 살아남을 수 있는 소만사의 저력에 존경을 표합니다. 척박한 우리나라 SW업계에 지속적으로 등대같은 역할을 해주시기 바랍니다. 소만사 "레알 살아있네~!" 〈공공 ○○님〉 쉽지 않은 길을 꾸준히 달려오고 지속적으로 발전하는 모습이 보기 좋습니다. 앞으로도 국가와 기업의 안전한 사이버환경을 위해 많은 노력을 부탁드리며 무궁한 발전을 기원합니다. 〈기업 ○○님〉 소중한 정보와 데이터 만년이라도 잘 지킬 수 있는 사람들에게 꼭 기억되는 보안솔루션 "소만사" 창립17년을 축하합니다. 〈병원 ○○님〉 소만사의 팬이 된지 이제 5년이 되었습니다. 나이로 치면 벌써 고등학생이네요. 가장 잘 하는 분야에서 긴 시간 집중하여 국내 보안의 새로운 지평을 연 점 정말 세계인들에게 자랑할 만 합니다. 앞으로도 가장 잘 하는 분야에서 최고의 기업으로 남길 진심으로 바랍니다. 〈기업 ○○님〉 소만사의 창립17주년을 축하드립니다. 앞으로도 대한민국의 보안을 책임지시길 바라고 뿌리깊은 나무가 바람에 흔들리지 않듯이 17년 동안 튼튼한 나무를 키웠듯이 앞으로의 소만사 미래는 튼튼할거라 기대합니다. 다시 한번 창립 17주년을 축하드립니다. 〈대학 ○○님〉 소만사의 창립 17주년을 축하합니다. 지난 17년간 국내 정보보호 수준향상을 위한 다양하고 효과적인 많은 솔루션들을 만들어 오시느라 고생하셨습니다. 앞으로 한걸음 더 나가기 위해 고객의 소리에 귀기울이고 고객의 필요가 잘 반영된 킬러 소프트웨어를 만들어

UnSung Hero(찬미되지 않는 영웅)는
박지성선수를 부르던 이름입니다.
자신을 숨기고 조직을 빛내는 영웅,
평상시에는 드러나지 않다가
위기가 오면 조직을 구해야 하는
헌신자를 말합니다.
바로 우리나라의 **보안담당자**들입니다.

2015년,
소만사와 2만여 보안담당자는
보안으로 한솥밥 19년차
가 되었습니다

내길 기대해 봅니다. 소만사 화이팅!! 〈보험 ○○님〉 소만사의 창립 17주년을 진심으로 축하드립니다. 강산이 한 번 변하고 또 다시 강산이 변하게 될 오랜 기간을 한우물만 파셨으니 우물물은 깊고 마르지 않는 정보보호의 물로 솟아나 개인정보를 위한 건강수가 되리라 믿습니다. 귀사가 개발한 Privacy-i로 개인정보보호를 위한 사업에 잘 활용하고 있습니다. 영세한 중(소)기업의 열악한 정보보호 강화를 위해서 도 소만사가 경제 적인 보안솔루션도 많이 보급하는데 선도기업이 되어 주시기를 기대합니다. 다시 한번 소만사의 창립 17주년을 축하 드립니다. 〈공공 ○○님〉 소만사의 창립 17주년 축하드립니다. 97년이면 대한민국 보안의 초창기 기업이네요. 사람나이 17살이면 질풍노도의 시기인 것처럼 앞으로 끊임없는 질주를 하시기를 바랍니다. 다시한번 축하드립니다. 화이팅~!! 〈증권 ○○님〉 소만사의 존재만으로 든든합니다. 17년차가 170년차가 되는 그날까지 늘 한결같이 대한민국의 대들보가 되어주세요. 응원합니다. 화이팅!! 〈기업 ○○님〉 소만사의 보안관련 참고 메일 소중히 잘보고 있습니다. 항상 정보보호에 대한 경각심도 깨우쳐 주시고 이렇게 17년차 보안 솔루션 회사가 되심을 축하드리고 100년이 넘는 기업으로 발전하시기를 성원드립니다. 감사합니다. 〈대학 ○○님〉 소만사의 17주년을 축하드리며 앞으로도 계속 (소)만사의 제품(만) (사)게되는 그런 S/W를 만들어 주시기 바랍니다. 〈기업 ○○님〉 소만사의 17년 생일을 축하합니다. 보안의 중요성이 날로 높아지는 지금 Local 기업에서 Global 기업으로 거듭나시길 기원합니다. 〈기업 ○○님〉 소만사와 인연을 맺은지도 벌써 5~6년이 지나가네요. 차세대 프로젝트와 함께 시작한 인연이었는데 그 때를 생각하면 감회가 새롭습니다. 창립 17년차 진심으로 축하드리며 오랫동안 소중한 사람들로 기억될 수 있는 그런 회사가 되기를 기원합니다. 〈증권 ○○님〉 어느새 열일곱살 청년(?)으로 의젓하게 성장한 소만사의 생일을 축하 드립니다! 지금까지 얼굴 그을려 가며 아궁이에 불 지펴서 한솥밥을 지어 오신 것처럼 이후로 더 맛있는 보안이라는 밥을 지을 수 있는 소만사가 되기를 응원합니다. 축하 드립니다!! 〈협회 ○○님〉 벌써 17년이라니 잘 몰랐지만 대단합니다. 100년 지속 기업으로 꼭 등재가 되었으면 합니다. 모든 사업이 번창하세요… 〈기업 ○○님〉 열 일곱번째 생일축하 드립니다. 열악한 환경에서도 어려움을 딛고 소프트웨어 만들기를 고집해온 장인정신과 일에 대한 열정!! 또한 내일을 위해 쌓은 역량들이 고객 가치는 높이고 오늘의 기쁨이 있지 않나 생각듭니다. 17주년 축하드리고 글로벌 기업으로 우뚝서기를 기원합니다. 〈교육 ○○님〉 와우~ 벌써 17년이나 됐군요. 오로지 보안솔루션 개발을 통한 회사의 발전... 30년 50년 꾸준히 발전하는 회사로 기억되길 기원합니다. 창립 17주년을 축하드립니다. 〈기업 ○○님〉 와우~~ 제가 소만사를 알게 된것이 약 7년전인것으로 기억하는데 이제보니 고3 졸업반이었군요… 축하합니다. 내년에는 성인이네요... 성인답게 더 큰 모습 기대하겠습니다... 축하드립니다~~ 〈병원 ○○님〉 우리나라 보안분야 역사와 함께 하신 소만사의 창립 17년차를 진심으로 축하드리며 폭발적인 보안분야 욕구에 더 큰 기여를 하실 것을 믿으며 앞날의 무궁한 발전을 기원합니다. 〈교육 ○○님〉 저희 회사와 인연을 처음 맺고 그 이후로도 필요한 솔루션이 있을 때마다 도움을 받은 소만사에 감사드리며 이제는 제가 팀을 이끄는 팀장이 되었지만 앞으로도 새로운 보안이슈를 해결해주는 소만사가 되어 저희 팀원에게 도움이 되었으면 합니다. 〈제약 ○○님〉 정보보안분야에서 17년 그 시간만큼 명사의 반열에 오른 소만사를 축하하며 축복해 드립니다. 앞으로도 발전하는 소만사를 기대하고 응원하겠습니다. 그리고 보안업계의 맏형으로도 많은 역할을 부탁드립니다. 진심으로 17살 소만사를 축하합니다. 〈교육 ○○님〉 지속 가능한 국내유일 보안기업으로 20년 50년 이상 지속적으로 보안 제품 혁신을 이루는 국내 보안을 책임져 줄 수 있는 1000억 이상 달성하는 보안 전문기업으로 성장하소서!! 〈기업 ○○님〉 창립 17주년 되심을 진심으로 축하드립니다. 이제는 청소년에서 청년으로 나아가는 사춘기시절이군요. 그동안 많은 경험들을 토대로 이 사춘기를 잘 이겨나가리라 믿습니다. 곧 성인이 될 소만사에 무한한 축하를 드립니다. 지금까지 잘 오셨듯이...이 기반을 더욱더 견고하게 만드셔서 훌륭한 성인으로 성장하기를 기원합니다. 감사합니다. 〈기업○○님〉 창립17년차시네요. 축하드립니다. 모든 임·직원분들이 힘을 모아 짧지도 길지도 않은 시간을 같이 보내오셨네요. 승승장구 화이팅하시길 바랍니다. 추카추카~!!! 〈증권 ○○님〉 창립17주년을 축하합니다. 소프트웨어를 만드는 전문가들이 만든 회사인 만큼 좋은 소프트웨어를 만들어 기업은 물론 국가적으로도 많은 기여를 하고 있는 것 같습니다. 올해는 국내뿐 아니라 해외로도 쭉쭉 성장해 나가길 기원합니다. 〈기업 ○○님〉 처음 소만사를 접하고 회사명의 뜻이 "소프트웨어를 만드는 사람"라는 걸 알았을 때 무척 신선했던 기억이 근 10여년 가까이 되어가는데도 아직까지 생생합니다.^^ 벌써 17년차라니 청소년을 거쳐 의젓한 청년이 될 시기인데 몸은 비록 17세 지만 이미 의식은 청년을 넘어 이미 성공한 어른이 된 듯합니다.^^ 앞으로 더욱 더 성장해가는 모습을 어떻게 보여 주실지 무척 기대됩니다. 다시 한번 열 일곱번째 생일 축하드립니다.^^ 〈기업 ○○님〉 17주년 너무 너무 축하드려요. 단일 분야에서 변치 않고 자리를 지켜 주셔서 감사합니다. 17주년 그 자체만으로도 신뢰가 갑니다. 더욱 번창하세요~ 〈기업 ○○님〉 17년차라니 너무 축하드립니다. 예전 소만사의 많은 자료들을 보고 세미나 참석도 많이 했지만 이렇게 오래될지는 저도 처음 알았네요.ㅎㅎ 17년된 소만사 앞으로 100년 200년 건승하기를 기원합니다. 앞으로 많은 발전 하세요. 〈교육 ○○님〉

"언제 사고날지 몰라서
자다가 깬다"

"희생양이
되겠구나 싶다"

"권한도 예산도 없이
책임만 진 처지가 서럽다"

"평소엔 불평하다가
사고나면 보안 탓하는
동료들이 무섭다"

"법이 자꾸 바뀌고 정확한 의미를
알기 어려워서
안개 속을 운전하는 기분이다 "

소만사는
보안담당자 한분한분이
매일 맞서야 하는
두려움을 압니다
19년간 겪어왔기 때문입니다

두려움의 원인은
복잡함과애매함이기에

소만사는
개인정보보호법규를
명확하게 풀어서
프라이버시레터로
공유해왔습니다

이 책은 7년간 이어져온
프라이버시레터를
2015년에 맞게
재분류, 수정하여 펴낸 것입니다

보안담당자분의 책상에 꽂혀서
업무에 조금이나마 도움이 된다면
더 바랄 나위가 없겠습니다

17년이나 되었군요. 귀사의 제품과 기술력으로 보아 앞으로도 지속적으로 성장할 수 있을 것 같습니다. 앞으로도 귀사의 무궁한 발전 기원합니다. 〈증권 ○○님〉 17년의 세월동안 회사가 유지되었다고 봐야 할꺼 같습니다. 이제까지 이끌어왔듯 앞으로도 좋은 지로 회사가 번창했으 면 좋겠습니다. 창립17주 년 다시한번 축하드립니 다. 〈기업 ○○님〉 17년동 안 한결같이 보안만 생각해온 소만사!!! 앞으로 170년 1700년... 한결같은 맘으로 더욱 보안에 힘써 주세요. 창립 17주년 축하 드립니다. 〈기업 ○○님〉 17년 동안 다른 것에 눈돌리지 않고 오로지 보안 그래서 훌륭한 제품들이 많이 나온 것 같습니다. 앞으로도 꾸준히 노력하여 대한민국 보안하면 소만사가 떠오로도록 더 많이 노력해 주세요. 〈연구원 ○○님〉 17년간 보안업계의 한 축을 담당해 오신 걸 축하드리며 앞으로도 보안의 발전에 기여하는 회사가 되시길 기원합니다. 〈기업 ○○님〉 SOMANSA의 17번째 생일을 진심으로 축하드립니다. 그룹 내 보안솔루션 구축에 있어 절대적인 역할을 충실히 해 주고 있어 정말 고맙게 생각합니다. 앞으로도 보안솔루션 업계 절대 강자의 위치를 굳건히 하고 무궁한 발전이 있기를 기원합니다. 〈기업 ○○님〉 행복합니다. 개인적으로 소만사와 인연이 벌써 15년째. 소만사의 주주가 아닌데도 소만사의 성장모습이 가슴 뿌듯합니다.^^ 어렵고 힘든 과정 잘 넘어가시고 한마음으로 성장하심에 박수를 보냅니다. 17년. 소만사! 무궁한 발전이 함께 하시길. 〈기업 ○○님〉 항상 앞선 통찰력과 혜안으로 보안시장을 선도해 나간 소만사의 17주년을 진심으로 축하드립니다. 지금까지는 우리나라의 보안시장을 개척하였다면 이제는 세계로 뻗어나가 글로벌 보안기업으로 우뚝 서시길 기원합니다. 다시 한번 소만사의 17주년을 축하드립니다^^ 〈기업 ○○님〉 축하합니다!!! 벌써 17년이 되었나요? 처음 만난 것이 1999년쯤이었던 것 같은데 끝까지 한우물만 파고 계시군요. 세계로 웅비하는 소만사의 도약과 전진을 기대합니다. 〈증권 ○○님〉 축하드립니다. 17년간 우리나라 전산 보안을 위하여 노력하신 소만사 임직원 여러분들의 노고에 고개가 숙여집니다. 앞으로 더 발전하시어 보안 분야의 제1위 기업이 되시길 바랍니다. 〈협회 ○○님〉 17주년을 진심으로 축하드립니다. 남들이 생각지 않을때 탁월한 선택으로 정보화사회의 보안 파수꾼이 걸어온길 평탄치 않았을것입니다. 보안이 선택이 아닌 필수가 되어버린 이 시대에 가장 필요한 "소만사" 다시 한번 진심으로 축하드립니다. 〈 〉 기업 ○○님 2002년 보안 업무를 맡으면서 굵직한 보안이슈가 나올때마다 적절한 솔루션을 제시해 주셨습니다. 보안인이라면 한솥밥의 의미에 공감을 느낄겁니다.축하드립니다 〈증권 ○○님〉강산이 두번 바뀌어갈 시간동안 한결같이 보안영역에서 독보적인 성과를 거두어 오신 것을 진심으로 축하 드립니다. 최근 해킹사건을 통해 보안의 중요성을 새삼 새롭게 느끼게 되는군요. 앞으로도 소만사 발전을 기원합니다 〈 공공 ○ ○ 님 〉 개인정보보호 17년차 소만사 축하드립니다!항상 무한발전하시길 바랍니다! 〈공공○○님〉 〈공공 ○ ○님〉 수많은 IT 보안 업계가 생겼다 사라지는 요즘 17년 동안 '보안' 을 이끌어온 소만사의 노고에 박수를 드립니다. 축하드립니다~ 앞으로도 '한국 보안'을 책임지는 회사가 되시길 바랍니다. 〈기업 ○ ○님〉 벌써 17년이 되었군요. 보안의 새로운 패러다임을 개척한 능력있는 회사. 정말 축하드립니다. 앞으로도 승승장구하는 창의력 있는 회사가 되었으면 합니다. 〈기업 ○ ○님〉 소만사 17년차를 축하합니다. 소프트웨어를 만드는 사람들이 뚜벅이처럼 한결같이 100년 200년차를 맞이하시기를 바랍니다. 〈기업 ○ ○님〉 소: 소문이 IT업계에 돌기 시작하더군요. 만: 만렙의 보안역량을 보유한 보안회사가 있다고. 사: 사실이었습니다. 소만사!! 창립 17주년 진심으로 축하드리며 앞으로도 우리나라 보안을 위해 쭉 달려가 주시길 바랍니다. 〈기업 ○ ○님〉한솥밥으로 한상 멋지게 차리시느라 고생 많으셨습니다. 한솥의 밥상을 차리기 위해 한톨 한톨의 쌀을 깨끗이 씻는 정성과 혁신과 열정으로 가마솥을 데우고 지금과 같은 세상이 올 때를 기다리며 뜸을 들이는… 앞으로 세계 보안시장의 패권을 쥘 수 있도록 한상 푸짐하게 먹으며 의기투합했으면 합니다. 다시한번 축하말씀 전합니다. 소만사... 파이팅!!!! 〈공공 ○ ○님〉