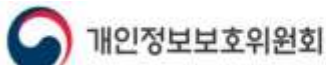


서귀포시자원봉사센터 CPO 및 개인정보취급자 대상

개인정보 보호 교육



Contents

1. 개인정보의 이해
2. 개인정보보호법의 체계
3. 개인정보의 처리 단계별 보호조치
4. 개인정보 침해사례 및 최신 동향
5. 개인정보의 기술적 · 관리적 보호조치
6. 사이버 공격과 정보보안 수칙

01

개인정보의 이해

1 개인정보의 이해



개인정보란?

개인에 대한 사실·판단·평가 등
개인에 관한 모든 정보



해당 정보만으로는
특정 개인을 식별할 수 없으나
다른 정보와 용이하게 결합하여
특정 개인을 식별 가능한 경우



1 개인정보의 이해



개인정보이다? 아니다?(1)

개인정보에 해당

- 사망자의 정보가 **유족과의 관계를 나타내는** 정보
- 유족 등의 **사생활을 침해**할 경우

“사망한 자에 관한 정보는
개인정보가 아니다!”

1

개인정보의 이해



개인정보이다? 아니다?(2)

개인정보에 해당

임원 및 업무 담당자 이름,
자택주소, 개인 연락처 등

“법인 또는 단체 정보는
개인정보가 아니다!”

법인 또는 단체의 이름, 소재지 주소,
대표 연락처(이메일 주소 또는 전화번호),
업무별 연락처, 영업실적

1 개인정보의 이해



관련 판례(1)

아이디와 비밀번호는?

아이디와 비밀번호는 개인정보에 해당할 수 있음

아이디와 비밀번호 등 식별부호는 실제 공간과는 달리 익명성이 통용되어 **행위자가 누구인지 명확하게 확인하기 어려운 가상공간에서 그 행위자의 인격을 표상**한다고 할 것이므로
(대법원 2005. 11. 25. 선고 2005도870 판결 참조) 개인에 관한 정보로서 당해 개인을 알아볼 수 있는 정보, 즉 정보통신망법 제2조 제1항 제6호에서 정한 개인정보에 해당함
(서울중앙지법 2007. 1. 26. 선고 2006나12182 참고)

이메일 주소는?

이메일 주소는 개인정보에 해당할 수 있음

이메일 주소는 당해 정보만으로는 특정 개인을 알아볼 수 없을지라도
다른 정보와 용이하게 결합할 경우 당해 개인을 알아볼 수 있는 정보라 할 것이므로
정보통신망법 제2조 제1항 제6호에서 정한 개인정보에 해당
(서울중앙지법 2007. 2. 8. 선고 2006가합33062, 53332 참조)



1 개인정보의 이해



관련 판례(2)

휴대전화번호 뒤 4자리는?

4자리만으로도 개인정보에 해당할 수 있음

휴대전화 뒷자리 4자만으로도 그 전화번호 사용자가 누구인지를 식별할 수 있는 경우가 있고, 특히 그 전화번호 사용자와 일정한 인적 관계를 맺어온 사람이라면 더욱더 그러할 가능성이 높으며, 설령 휴대전화번호 뒷자리 4자만으로도 그 전화번호 사용자를 식별하지 못한다 하더라도 그 뒷자리 4자와 관련성이 있는 다른 정보(생일, 기념일 등)와 쉽게 결합하여 그 번호 사용자가 누구인지를 알아 볼 수도 있다...개인정보보호법 제2조 제1호에 규정된 개인정보에 해당된다.

(대전지법2013.8.9.선고 2013고단17판결)

휴대전화의 IMEI는?

휴대전화의 IMEI는 개인정보에 해당할 수 있음

휴대전화마다 하나씩 부여된 USIM 일련번호와 IMEI(국제모바일 단말기 인증번호)도 개인정보에 해당. 어느 개인의 소유로 귀속되는 순간부터 이 번호들은 기계 고유번호라는 의미 외에 개인이 소유하는 휴대전화의 일련번호라는 의미를 함께 지니게 되고 가입자정보에 나타난 개인정보 와도 쉽게 결합해 개인을 특정할 수 있기 때문에 개인정보에 해당한다.



1 개인정보의 이해



개인정보의 유형과 분류



1 개인정보의 이해



현대 사회에서의 개인정보의 가치



개인의 인권

개개인의 사회관계,
권리를 나타내는 인권적 가치
(개인정보 자기결정권)



기업의 영업자산

고객의 정보를 수집·활용하여
영업활동 및 수익창출
개인정보 보호를 위한 노력은
비용이 아닌 투자



사회의 핵심요소

공공·민간 서비스, 기업경영 등
대부분의 사회 활동이
개인정보를 기반으로 이루어짐

1 개인정보의 이해



개인정보 자기결정권 – 개인정보에 대한 인식



과거 소극적 개념

개인의 사적인 생활을
남에게 방해 받지 않을 권리
(Privacy)



DO NOT
DISTURB



현재 적극적 개념

개인정보의 경제적·사회적
가치가 증가함에 따라
개인은 자신에 관한 정보를
적극적으로 관리·통제



개인정보 자기결정권

(Self control on Personal Information)

자신에 관한 정보가 언제, 어떻게, 어느 범위까지
수집, 이용, 공개될 수 있는지를
정보주체가 스스로 통제, 결정할 수 있는 권리

02

개인정보보호법의 체계

2 개인정보보호법의 체계



용어 정리(1)

개인정보

- 성명, 주민등록번호 및 영상 등을 통하여 살아있는 개인을 알아볼 수 있는 정보
- 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보
- 별도로 보관된 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보

※ 개인정보 보호법은 임직원, 주주, 협력업체 등 모든 사람의 개인정보에 적용됨

정보주체

- 처리되는 정보에 의해 알아볼 수 있는 그 정보의 주체가 되는 사람

개인정보 파일

- 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)

처리

- 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위

2 개인정보보호법의 체계



용어 정리(2)

개인정보 처리자

- 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체, 개인 등

개인정보 보호 책임자

- 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자

개인정보 취급자

- 개인정보처리자의 지휘감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등

개인정보 처리시스템

- 데이터베이스 시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 응용시스템

영상정보 처리기기

- 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유무선망을 통하여 전송하는 장치, 폐쇄회로 텔레비전, 네트워크 카메라

2 개인정보보호법의 체계



개인정보 보호 원칙 (제3조)

- 1》 처리 목적의 명확화, 목적 내에서 적법하고 정당하게 최소 수집
- 2》 처리 목적 내에서 처리, 목적 외 활용 금지
- 3》 처리 목적 내에서 정확성·완전성·최신성 보장
- 4》 정보주체의 권리침해 위험성 등을 고려하여 안전하게 관리
- 5》 개인정보 처리사항 공개, 정보주체의 권리보장
- 6》 사생활 침해 최소화 방법으로 처리
- 7》 익명처리가 가능한 경우 익명으로 처리
- 8》 개인정보처리자의 책임 준수, 정보주체의 신뢰성 확보



2 개인정보보호법의 체계



정보주체의 권리 (제4조)

- 1》 개인정보의 처리에 관한 정보를 **제공받을 권리**
- 2》 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 **선택, 결정할 권리**
- 3》 개인정보의 처리 여부 확인, 개인정보 **열람을 요구할 권리**
(사본 발급 포함)
- 4》 개인정보의 **처리 정지, 정정·삭제 및 파기를 요구할 권리**
- 5》 개인정보의 처리로 인한 **피해를 신속, 공정하게 구제받을 권리**

개인정보 자기결정권

자신에 관한 정보가 언제, 어떻게, 어느 범위까지 수집, 이용, 공개될 수 있는지를 정보주체가 스스로 통제, 결정할 수 있는 권리

2 개인정보보호법의 체계



개인정보 보호법은 **일반법** (6조)

개인정보 보호법은 개인정보 보호 분야의 일반법

- » 사회 전반의 개인정보 보호를 규율
- » 모든 공공기관, 사업자, 법인, 단체, 개인 등

다른 법률에 특별한 규정이 있는 경우

- » 해당 법률의 규정을 우선 적용
 - ※ **자원봉사활동기본법**, 신용정보보호법, 의료법 등



2 개인정보보호법의 체계



개인정보보호법의 체계

개인정보 보호법 총칙(1장)

- ▶ 개인정보의 정의
- ▶ 개인정보 보호 원칙
- ▶ 정보주체의 권리
- ▶ 다른 법률과의 관계

개인정보의 처리(3장)

- ▶ 개인정보 수집, 이용, 제공
 - 개인정보 수집·이용, 제공
 - 목적 외 이용·제공 제한, 파기
- ▶ 개인정보 처리 제한
 - 주민등록번호, 고유식별정보, 민감정보 처리 제한
 - 영상정보처리기기 설치·운영 제한

정보통신서비스제공자 특례(6장)

- ▶ 수집·이용, 파기 등 특례
- ▶ 개인정보 이용내역 통지
- ▶ 손해배상의 보장
- ▶ 국내대리인 지정

개인정보의 안전한 관리(4장)

- ▶ 안전조치 의무
 - 관리적, 기술적, 물리적 보호조치
- ▶ 보호책임자 지정, 처리방침 공개
- ▶ 유출 시 조치 해야 할 사항
 - 통지 및 신고, 대책 수립 및 시행

권리 보장 및 구제(5·7·8장)

- ▶ 정보주체의 권리 보장
 - 열람, 정정, 삭제, 처리 정지, 손해배상 등
- ▶ 개인정보 분쟁조정
 - 조정의 신청, 절차 등
- ▶ 단체소송
 - 단체소송 대상, 절차 등

2 개인정보보호법의 체계



개인정보 보호 관련 법 체계 (2020년 2월 이전)

	정보통신	금융	개인정보 보호 일반
소관법령	정보통신망 이용촉진 및 정보보호 등에 관한 법률	신용정보의 이용 및 보호에 관한 법률	개인정보 보호법
적용범위	정보통신서비스 제공자가 이용자 개인정보 수집 시	신용정보업자 등이 개인신용정보 수집·활용·제공 시	개인정보취급자가 정보주체 개인정보 수집 시
적용대상	- 정보통신서비스 제공자 등 - 방송사업자 - 수탁자	- 신용정보집중기관(5개) - 신용정보업자(33개) - 기타 신용정보처리 개인정보취급자 등	오프라인 사업자, 근로자, 비영리단체(협회, 동창회 등), 공공기관 등
수집	- 수집 목적 등 고지 및 사전동의 획득 후 수집 - 주민번호 수집 제한	- 수집 시 목적 명확 - 합리적·공리적 수집 - 신용정보 무관 정보 수집 금지	- 수집 목적 등 고지 및 사전동의 획득 후 수집 - 주민번호 수집 제한
이용/제공	목적 외 이용 및 동의 없는 제3자 제공 금지	- 개인신용정보 제공 및 활용 시 동의 획득 의무 - 상거래 관계 설정·유지 여부 판단 외 제공 금지	목적 외 이용 및 동의 없는 제3자 제공 금지

2 개인정보보호법의 체계



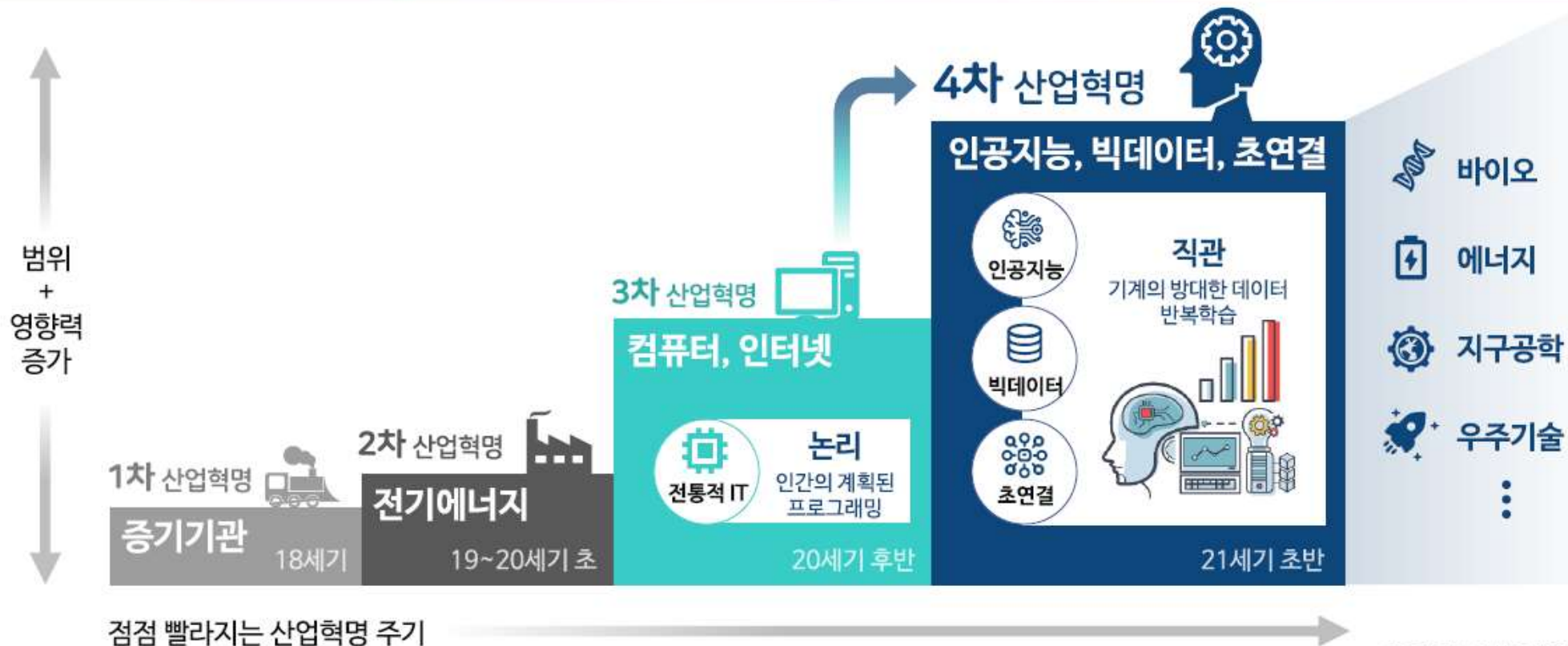
4차 산업혁명의 중요성과 개인정보의 보호·활용의 필요성 대두

4차 산업혁명시대와
신산업 육성의 필요성 대두

신기술을 활용한 데이터 이용과
그에 따른 사회적 규범의
정립 필요

개인정보 활용의 한계 및
관련 법령의 체계적 정비 필요

개인정보 보호법 개정



2 개인정보보호법의 체계



개인정보보호법 개정 목적과 주요 내용(1)

개정 목적

- ✓ 데이터 기반의 신산업 육성과 양질의 일자리 창출에 기여
- ✓ 개인정보 보호체계의 일원화와 체계적 정책 추진
- ✓ EU GDPR 적정성 평가를 위한 감독기구의 독립성 확보



주요 내용

가명정보의 도입과 데이터 활용 제고

개인을 알아볼 수 없도록 한 안전하게 처리된 가명정보의 도입

동의없이 처리 가능한 개인정보 합리화

수집목적과 합리적으로 관련된 범위 내에서 개인정보 이용, 제공 허용

개인정보의 범위 명확화

개인정보는 특정 개인을 알아 볼 수 있는 정보의 판단기준 신설

개인정보 보호체계의 일원화

감독기구 일원화, 법 체계 일원화

2 개인정보보호법의 체계



개인정보보호법 개정 목적과 주요 내용(2)

개정 목적

- ✓ 정보통신망법 내 개인정보 관련 다른 법령과의 유사·중복조항 정비
- ✓ 개인정보보호를 위한 협치 (거버넌스) 개선

주요 내용

개인정보보호 관련 사항 개인정보 보호법으로 이관

온라인상 개인정보 보호 관련 규제와 감독 주체
〈개인정보보호위원회〉로 변경

정보통신망법에 규정된 개인정보 보호에 관한 사항을
「개인정보 보호법」으로 이관

온라인상의 개인정보 보호와 관련된 규제와 감독의 주체를
방송통신위원회에서 〈개인정보보호위원회〉로 변경

2 개인정보보호법의 체계



개인정보보호법 개정 목적과 주요 내용(2)

개정 목적

- ✓ 정보통신망법 내 개인정보 관련 다른 법령과의 유사·중복조항 정비
- ✓ 개인정보보호를 위한 협치 (거버넌스) 개선

주요 내용

개인정보보호 관련 사항 개인정보 보호법으로 이관

온라인상 개인정보 보호 관련 규제와 감독 주체
〈개인정보보호위원회〉로 변경

정보통신망법에 규정된 개인정보 보호에 관한 사항을
「개인정보 보호법」으로 이관

온라인상의 개인정보 보호와 관련된 규제와 감독의 주체를
방송통신위원회에서 〈개인정보보호위원회〉로 변경

2 개인정보보호법의 체계



정보통신망법과 개인정보보호법의 통합

개정 이전

개인정보보호법
(일반법)

정보통신망법
(특별법)



개정 이후

개인정보보호법

정보통신 관련
특례조항 포함



개인정보보호법으로 흡수 · 통합

- 동의받는 방법
- 민감정보의 처리
- 개인정보 처리 위탁
- 영업의 양도 · 양수
- 개인정보 보호책임자
- 인증
- 열람 · 정정 · 삭제 요구
- 손해배상
- 법정 손해배상
- 금지 행위
- 고발



기존 규정 개정

- 개인정보 제공
- 목적 외 이용 / 제공 제한



특례 이관

- 수집 · 이용
- 유출 통지 및 신고
- 개인정보 유효기간제
- 동의 철회
- 이용 내역 통지
- 손해배상 보험
- 노출 개인정보 삭제 · 차단
- 국내 대리인
- 국외 이전
- 상호주의
- 과징금
- 방송사업자 준용

2 개인정보보호법의 체계

개인정보 보호 감독기구의 일원화



개인정보보호 관련 업무를 보호위원회로 통합·이관



2 개인정보보호법의 체계



가명정보의 도입을 통한 데이터 이용 활성화



개인정보

특정 개인에 관한 정보,
개인을 알아볼 수 있게 하는 정보

예) 홍길동, 32살, 남성, 서울시,
마포구 공덕동, 010-1234-5678



가명정보

추가정보의 사용 없이는 특정
개인을 알아볼 수 없도록 한 정보

예) 홍xx, 32살, 남성, 서울시,
마포구, 010-xxxx-xxxx



익명정보

더 이상 개인을
알아볼 수 없도록 한 정보

예) 서울 사는 30대 남성



가명정보

원래의 상태로 복원하기 위한 추가 정보의 사용 결합 없이는
특정 개인을 알아볼 수 없는 정보



가명처리

개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는
등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수
없도록 처리하는 것 (개인정보보호법 개정 제2조)



가명정보의 처리

① 통계작성, ② 과학적 연구, ③ 공익적 기록보존 등의

목적으로 정보주체의 동의 없이 가명정보 처리 가능

(개인정보보호법 개정 제28조의2(가명정보의 처리 등))

2 개인정보보호법의 체계

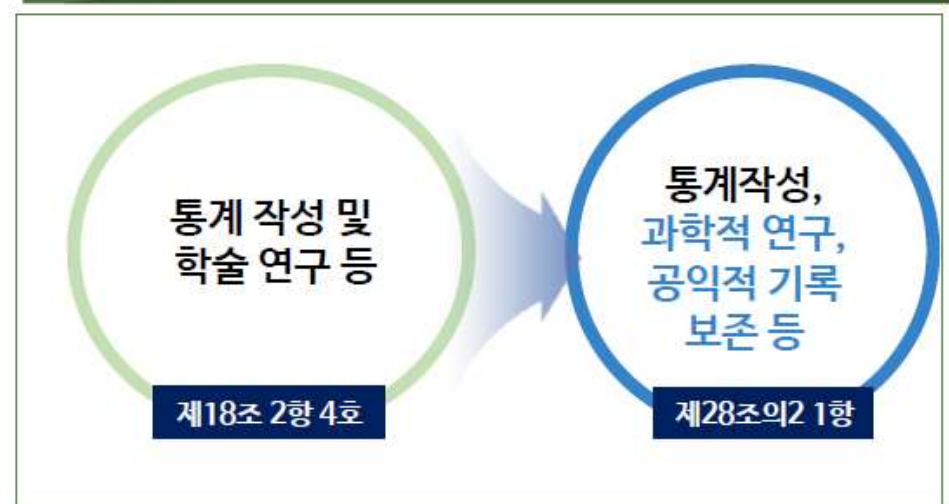


데이터의 이용 제공 범위 확대

개인정보의 이용·제공 범위 확대



가명정보의 이용·제공 범위 확대



고려사항

- (수집목적) 당초 수집 목적과의 합리적 관련 범위
- (정보주체) 정보주체의 불이익 발생 여부
- (안전성 확보조치) 암호화 등 안전성 확보조치 등

가명정보 이용·제공 범위

- 과학적 연구, 통계작성, 공익적 기록보존 등
- 新기술·제품·서비스 개발 등 산업적 목적을 포함하는 과학적 연구, 시장조사와 상업 목적의 통계 작성도 포함

2 개인정보보호법의 체계



(동의없이) 개인정보 이용 제공 기준 추가

기 존

법률에서 위임한 사항에 대한 규정

개 정

개인정보 이용·제공 조건



(동의없이) 개인정보 이용·제공 기준 추가

- 개인정보 수집 목적 범위 내에서만 이용 가능
- 수집 목적 변경 시 정보주체의 별도 동의 필요

- 당초 수집 목적과 관련성 존재 여부
 - 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부
 - 정보주체의 이익을 부당하게 침해하는지 여부
 - 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부
- ★ 판단 기준을 개인정보 처리방침에 미리 공개

2 개인정보보호법의 체계



민감정보의 범위 변경

기 존

민감정보의 범위

- 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보
- 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보
 1. 유전자검사 등의 결과로 얻어진 유전정보
 2. 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보

개 정

민감정보의 확대

- 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보
- 인종이나 민족에 관한 정보

변화하는 사회·기술 환경과 EU 등 국제적 환경에 맞는 개인정보의 보호

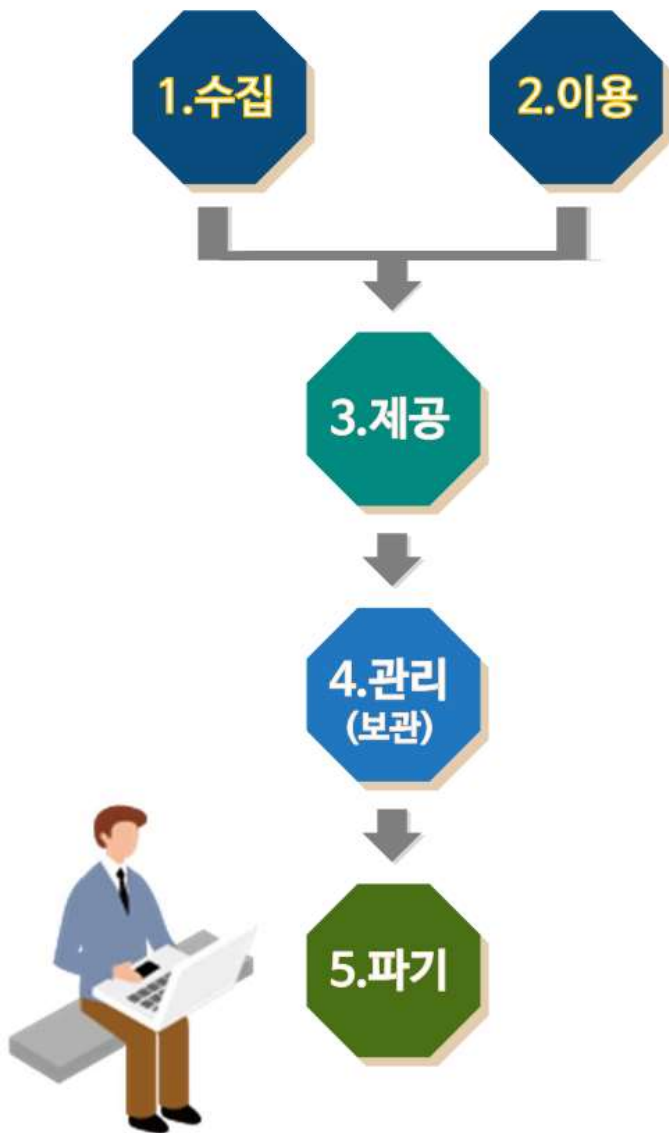
03

개인정보보호의 처리

3 개인정보의 처리



개인정보 처리단계별 보호조치



수집·이용 (15조)

최소 수집 (16조)

14세미만법정대리인동의 (22조)

- 처리제한 -
민감정보 (23조)
고유식별정보 (24조)
주민등록번호 (24조의 2)

제3자 제공 (17조)

목적외이용·제공제한 (18조)

처리위탁 (26조)

국외이전 (17조)

영업양도·양수 (27조)
(민간)

안전조치 의무 (29조)

처리방침 (30조)
보호책임자 (31조)

개인정보유출 통지·신고 (34조)

개인정보파일 등록 (32조)
(공공기관)

파기 (21조)



3 개인정보의 처리



개인정보의 수집·이용 (1)

※ 민감정보, 고유식별정보, 주민등록번호는 제15조, 제17조, 제18조 해당 없음!

1. 정보주체의 동의를 받은 경우

※ 동의를 받을 때 고지 의무 사항 (위반 시 3천만원 이하의 과태료)

- ① 수집·이용 목적 ② 수집 항목 ③ 보유·이용 기간
- ④ 동의 거부 권리 및 동의거부 시 불이익 내용

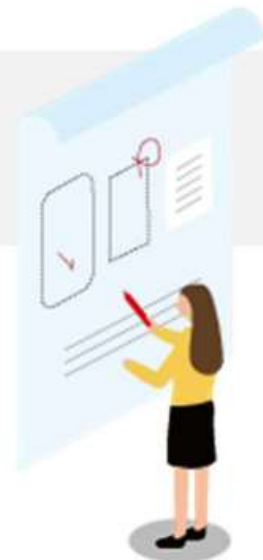
2. 법률의 특별한 규정, 법령상 의무 준수를 위해 불가피한 경우

3. 공공기관이 법령 등에서 정한 소관업무를 위해 불가피한 경우

4. 정보주체와의 계약 체결·이행에 불가피한 경우

5. 명백히 정보주체 등의 급박한 생명, 신체, 재산의 이익을 위해 필요한 경우

6. 개인정보처리자의 정당한 이익 달성을 위해 필요한 경우로서,
명백하게 정보주체의 권리보다 우선하는 경우



위반 시 ➡ 5천만원 이하의 과태료

3 개인정보의 처리



개인정보의 수집·이용 (2)

Q

정부기관에서 정책홍보 퀴즈이벤트를 진행하는데
참여자의 개인정보(성명, 연락처)를 수집하면서
동의 여부(예, 개인정보수집에 동의합니다.)에 대한 확인만
요청해도 되나요?



A

개인정보 수집·이용 시 개인정보의 수집·이용 목적, 수집하려는 개인정보의 항목,
개인정보의 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에
따른 불이익이 있는 경우 그 불이익의 내용을 알리고 이벤트 참여자의 동의를 받아야
합니다. 따라서 개인정보 취득 동의 여부만을 확인하고 고지사항의 전부 또는 일부를
알리지 않았다면 적법한 정보주체의 동의가 있었다고 보기 어렵습니다.

3 개인정보의 처리



동의 받는 방법 (1)

- ▶ 정보주체(법정대리인 포함)의 동의를 받을 때에는 각각의 동의사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 함
- ▶ 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분
 - 개인정보의 수집·이용, 개인정보의 제3자 제공, 민감정보의 처리, 고유식별정보의 경우
 - 동의 없이 처리 가능한 개인정보라는 입증책임은 개인정보처리자에게 있음
- ▶ 홍보나 마케팅 등의 이유로 개인정보 처리 동의를 받으려 할 때는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 함
- ▶ 선택적으로 동의할 수 있는 사항을 동의하지 않는다는 이유로 재화 또는 서비스의 제공 거부 금지(위반 시 3천만원 이하의 과태료)
- ▶ 만 14세 미만 아동의 개인정보를 처리하려면 법정대리인의 동의를 받아야 함(위반 시 5천만원 이하의 과태료)
 - 법정대리인의 동의를 받기 위해 필요한 최소한의 정보(성명, 연락처)는 해당 아동으로부터 직접 수집할 수 있음



3 개인정보의 처리



동의 받는 방법 (3)

동의서에 명확히 표시하여야 하는 사항

- ▶ 재화나 서비스의 홍보 및 판매 권유 등을 위해서 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실
- ▶ 개인정보 중 다음의 사항
- 민감정보, 여권번호, 운전면허번호, 외국인등록번호
- ▶ 개인정보의 보유 및 이용 기간
(제공 시에는 제공받는 자의 보유 및 이용기간)
- ▶ 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적



★ 표시 방법 ★

- ▶ 글씨는 9포인트 이상의 크기로 하되 다른 내용보다 20% 이상 크게 할 것
- ▶ 다른 색의 글씨, 굵은 글씨 또는 밑줄 등을 사용하여 명확히 드러나게 할 것
- ▶ 중요한 내용이 많은 경우에는 별도로 요약하여 제시할 것

3 개인정보의 처리



개인정보의 수집·이용·제3자 제공 동의서

참고

현장체험학습을 위한 개인정보 수집 · 이용 및 제공 동의서(예시)

본교는 2015년 ○월 ○○일 실시할 예정인 현장체험학습과 관련하여 아래와 같이 개인정보를 수집·이용 및 제3자에게 제공하고자 합니다. 내용을 자세히 읽으신 후 동의 여부를 결정하여 주십시오.

□ 개인정보 수집 이용 내역

항목	수집목적	보유기간
학생의 성명, 학년, 반, 전화번호, 학부모 성명, 전화번호	현장체험학습 운영	1년

※ 위의 개인정보 수집·이용에 대한 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 원활한 현장체험학습에 제한을 받을 수 있습니다.

☞ 위와 같이 개인정보를 수집·이용하는 데 동의하십니까? ☐ 동의 ☐ 미동의

□ 민감정보 처리 내역

항목	수집목적	보유기간
질병명, 감염 기간, 질병 감염 경로	학생의 위생 관리	1년

※ 위의 민감정보 처리에 대한 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 원활한 현장체험학습에 제한을 받을 수 있습니다.

☞ 위와 같이 민감정보를 처리하는 데 동의하십니까? ☐ 동의 ☐ 미동의

□ 개인정보 제3자 제공 내역

항목	제공 목적	제공하는 항목	보유기간
○○군부대	현장체험학습장 출입자 신분 확인	학생의 성명, 학년, 반, 전화번호	1년

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 원활한 현장체험학습에 제한을 받을 수 있습니다.

☞ 위와 같이 개인정보를 제3자 제공하는 데 동의하십니까? ☐ 동의 ☐ 미동의

<기타 고지 사항>

개인정보 보호법 제15조 제1항 제3호에 따라 정보주체의 동의 없이 개인정보를 수집·이용합니다.

개인정보 처리 사유	개인정보 항목	수집 근거
학사관리	학생의 성명, 생년월일, 주소, 보호자 성명, 생년월일	『초·중등교육법』 제25조 『학교생활기록의 작성 및 관리에 관한 규칙』

년 월 일

본인 성명 (서명 또는 인)
법정대리인 성명 (서명 또는 인)

3 개인정보의 처리



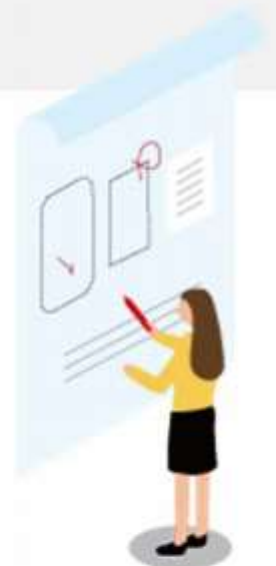
개인정보의 수집 제한

※ 민감정보, 고유식별정보, 주민등록번호는 제15조, 제17조, 제18조 해당 없음!

▶ 필요 최소한의 개인정보 수집

※ 정보주체의 동의를 받거나 법령의 처리 근거 또는 계약의 체결·이행 등을 위해 불가피하게 개인정보 수집하는 경우에도 처리 목적 달성에 필요한 최소한의 개인정보만을 수집

- ▶ 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담
- ▶ 필요 최소한의 정보 외의 개인정보 수집에는 동의 거부 가능
- ▶ 최소한의 개인정보 이외의 개인정보 수집에 동의하지 않는다는 이유로 재화 등 제공 거부 금지 (위반시 3천만원 이하의 과태료)



3 개인정보의 처리



개인정보의 수집 제한

“ **민감정보 및 고유식별정보는 원칙적으로 처리 금지** ”

정보주체에게 **별도 동의**를 얻거나, **법령에서 구체적으로**
처리를 요구하거나 허용하는 경우에 한하여 처리

민감정보

사상, 신념, 노동조합·정당가입,
건강정보, 유전정보, 범죄경력 정보

고유식별정보

주민등록번호, 여권번호,
운전면허번호, 외국인등록번호

위반 시 ➡ 5년 이하의 징역 또는 5천만원 이하의 벌금

분실·도난·유출·위조·변조·훼손되지 않도록
안전성 확보조치 의무 (위반 시 3천만원 이하의 과태료)

위 규정에도 불구하고 **주민등록번호는 법률 또는 대통령령 등에**
구체적으로 처리근거가 있어야 처리가 가능함(제24조2)



3 개인정보의 처리



개인정보의 위탁 (1)

알쏭달쏭, 개인정보 처리 업무 위탁일까? 제3자 제공일까?

구분	업무 위탁(법 제26조)	제3자 제공(법 제17조)
개인정보 제공 목적	위탁자의 이익을 위함	제3자의 이익을 위함
처리 방법	정보주체 동의 없이, 위·수탁 계약에 의해 처리하고, 위탁사실을 공개	정보주체의 동의를 받아 처리 ※ 법 제17조1항2호 예외
관리·감독 의무	위탁자	제공받는 자
손해배상 책임	위탁자 및 수탁자 부담	제공받는 자 부담
예시	홈페이지 관리, 대행업체 (입시원서, 졸업앨범, 대학등록금, 수학여행 등)	청렴도 조사(공공기관 → 권익위), 병무행정업무(학교 → 병무청) 등

※ 개인정보의 '처리위탁' 은 본래의 개인정보 수집, 이용 목적과 관련된 위탁자 본인의 업무처리와 이익을 위하여 개인정보가 이전되는 경우를 의미
(대법원 2017. 4. 7. 선고 2016도13263)

3 개인정보의 처리



개인정보의 위탁 (2)

 업무 위탁, 이것만은 꼭 기억하세요!

계약 전

01

▶ 위·수탁 문서 작성* ※ 위반 시 1천만원 이하의 과태료

* 필수항목 : 위탁업무의 목적 및 범위, 목적 외 개인정보 처리 금지, 안전성 확보 조치, 재위탁 제한, 관리점검 등 감독, 손해배상 책임

업무 수행 중

02

▶ 위탁사항 공개*(홈페이지, 관보 등) ※ 위반 시 1천만원 이하의 과태료

* 단, 마케팅 위탁의 경우 서면등의 방법(전자우편, 전화 등)으로 고지

▶ 수탁자 교육 및 감독

업무 종료 후

03

▶ 개인정보의 파기(5일 이내)·반환 및 결과 확인

3 개인정보의 처리



개인정보 수집 목적 범위 내 제3자 제공 (1)

※ 민감정보, 고유식별정보, 주민등록번호는 제15조, 제17조, 제18조 해당 없음!

1. 정보주체의 동의를 받은 경우

※ 동의 받을 때 고지 의무 사항 (위반 시 3천 만원 이하의 과태료)

- ① 개인정보를 제공받는 자 ② 제공받는 자의 개인정보 이용 목적
- ③ 제공하는 개인정보의 항목 ④ 제공받는 자의 개인정보 보유·이용기간
- ⑤ 동의거부 권리 및 동의거부 시 불이익 내용



2. 다음에 경우에 따라 수집한 목적 범위 내에서 제공하는 경우

- 법률의 특별한 규정, 법령상 의무 준수를 위해 불가피한 경우
- 공공기관이 법령 등에서 정한 소관업무를 위해 불가피한 경우
- 명백히 정보주체 등의 급박한 생명, 신체, 재산의 이익을 위해 필요한 경우

위반 시 ➡ 5년 이하의 징역 또는 5천만원 이하의 벌금

3 개인정보의 처리



개인정보 수집 목적 범위 내 제3자 제공 (2)

사례

1. 법률의 특별한 규정

- ▶ 「보험업법」 제176조에 따라 보험요율산출기관은 보험계약자의 교통법규 위반 정보를 제공받아 보험회사가 보험료 산출에 이용하도록 제공

2. 법령상 의무 준수

- ▶ 「학원의 설립·운영 및 과외교습에 관한 법률」 제6조에 따른 학원의 설립·운영하려는 자의 강사명단 등을 교육감에게 등록 의무
- ▶ 「소득세법」 제127조 및 제128조에 따른 소득지급자의 소득 귀속자의 대한 원천징수의무 및 원천징수 이행상황신고 등 이행

3. 공공기관이 법령 등에서 정한 소관업무를 위해 불가피한 경우

- ▶ 「정부조직법」 및 각 기관별 직제령·직제규칙, 개별 조직법 등에서 정하고 있는 소관사무 「주민등록법」, 「의료법」, 「국민건강보험법」 등 개별 법에서 정하고 있는 소관사무

3 개인정보의 처리



개인정보 수집 목적 외 이용 · 제3자 제공 (1)

※ 민감정보, 고유식별정보, 주민등록번호는 제15조, 제17조, 제18조 해당 없음!

목적 외 이용·제공은 원칙적으로 금지, 다만 아래 사항 중
정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 없는 경우 예외적 허용

1. 정보주체의 별도 동의를 받은 경우
2. 다른 법률의 특별한 규정이 있는 경우
3. 명백히 정보주체 또는 제3자의 생명, 신체, 재산의 이익에 필요한 경우
4. 통계작성 및 학술연구 목적에 필요한 경우로 특정 개인을 알아볼 수 없는 형태로 제공하는 경우

공공기관만 해당

5. 개인정보를 목적 외로 이용하거나 제3자에게 제공하지 않으면 다른 법률에서 정하는 소관업무 수행 불가능한 경우로 개인정보보호위원회의 심의·의결을 거친 경우
6. 조약, 국제협정 이행을 위해 외국정부 등 제공에 필요한 경우
7. 범죄수사 및 공소제기·유지 8. 법원의 재판업무 수행 9. 형 및 감호, 보호처분 집행

위반 시 ➡ 5년 이하의 징역 또는 5천만원 이하의 벌금

3 개인정보의 처리



개인정보 수집 목적 외 이용 · 제3자 제공 (2)

사례

1. 다른 법률의 특별한 규정 사례

- 「소득세법」 제170조에 따른 세무공무원의 납세의무자 등에 대한 조사, 질문
- 「감사원법」 제27조에 따른 감사원의 감사 관계자 등 자료 요구
- 「국가유공자 등 예우 및 지원에 관한 법률」 제77조에 따른 국가 유공자 등록 등을 위하여 국가보훈처장이 관계기관의 장에게 가족관계 등록사항 등에 자료제공 요구
- 「병역법」 제81조제2항에 따른 병무청장이 병역 이행 사항 확인·점검을 위하여 지방자치단체 등의 자료제공 요구
- 「부패방지 및 국민권익위원회 설치와 운영에 관한 법률」 제42조제1항 및 제3항에 따른 국민권익위원회가 민원사항에 대한 조사를 위해 관계기관에 자료제출 요구 등

3 개인정보의 처리



개인정보 수집 목적 외 이용 · 제공에 따른 이행사항



공공기관 이행사항

- 개인정보 이용 및 제공 관련 법적 근거, 목적 및 범위 관련 사항을 관보 또는 인터넷 홈페이지 게재
- 개인정보 목적 외 이용 및 제3자 제공 대장 기록 관리



3 개인정보의 처리



개인정보 제3자 제공에 따른 이행사항(2)

01

먼저 정보주체에게 별도 동의를 받거나, 법적 근거를 확인 합니다.

개인정보를 제공 할 때에는 반드시 정보주체에게 별도 동의를 받거나, 법령 근거를 확인 하여야 합니다.

필수 고지사항

- ① 개인정보를 제공 받는 자
- ② 제공받는 자의 개인정보 이용 목적
- ③ 이용 제공하는 개인정보의 항목
- ④ 개인정보의 보유 이용 기간
- ⑤ 동의거부 권리와 불이익

법적근거

- ① 정보주체에게 별도의 동의를 받은 경우(17, 18조)
- ② 법률에 특별한 규정이 있는 경우(17, 18조)
- ③ 소관 업무를 수행을 위하여 불가피할 경우(17조)



개인정보 보호책임자의 승인을 받습니다.

02

개인정보를 목적 외 이용 · 제공 할 때에는 반드시 개인정보 보호책임자에게 승인을 받으셔야 합니다.



※ 개인정보를 목적 외 이용 · 제공 할 때에는 대장에 기록하여 관리

3 개인정보의 처리



개인정보 제3자 제공에 따른 이행사항 (3)

03

‘제공받는 자’에게 보호조치 요구를 합니다.

개인정보를 제공받는 자에게 이용 목적·방법·기간·형태 등을 제한하거나, 안전성 확보에 필요한 조치를 마련하도록 문서로 요청 하여야 합니다.



개인정보 제공 후 주요내용은 공개 합니다.

개인정보를 목적 외 이용·제공하는 경우에는 이용·제공 한 날로부터 30일 이내 관보 또는 홈페이지에 10일 이상 계속 게재 하여야 합니다.

04

개인정보의 **제공**은 적법한 절차를 준수 하여야 합니다

3 개인정보의 처리



개인정보의 수집 출처 등 고지

- ▶ 정보주체 이외로부터 수집한 개인정보를 처리할 때, 정보주체의 요구가 있으면 즉시(3일 이내) 다음의 사항을 알려야 함 (위반 시 3천만원 이하의 과태료)

- 개인정보 수집 출처, 개인정보 처리 목적, 개인정보 처리 정지를 요구할 권리가 있다는 사실

- ▶ 일정 기준 이상의 개인정보처리자는 제3자로부터 개인정보를 제공받은 경우 정보주체에게 수집 출처, 처리목적, 처리정지 요구가 가능함을 고지하여야 함 (위반 시 3천만원 이하의 과태료)

※ 단, 정보주체에게 알릴 수 있는 개인정보(연락처 등)가 없다면 적용 제외 가능

- ▶ 고지의무 대상 개인정보처리자

- 5만명 이상의 민감정보 또는 고유식별정보를 처리하는 자
- 100만명 이상의 정보주체에 대한 개인정보를 처리하는 자

- ▶ 고지 방법 및 시기

- 서면, 전화, 문자전송, 전자우편 등 방법으로 개인정보를 제공받은 날로부터 3개월 이내
- 정보주체의 동의를 받은 범위에서 연 2회 이상 주기적으로 제공받는 경우 제공 받은 날로부터 3개월 이내 또는 동의를 받은 날로부터 기산하여 연 1회 이상

- ▶ 고지하였다는 사실, 알린 시기, 알린 방법을 개인정보 파기할 때까지 보관 관리

- ▶ 단, 범죄수사, 공소 제기·유지, 형·감호 집행, 교정·보호·보안관찰 처분, 출입국 관리사항 등의 개인정보, 다른 사람의 생명·신체를 해할 우려 또는 재산·이익의 부당한 침해 우려 시에는 적용 예외

3 개인정보의 처리



개인정보의 파기 (1)

- ▶ 보유기간의 경과, 처리목적 달성 등 개인정보가 불필요하게 되었을 때
지체 없이(5일 이내) 파기(위반 시 3천만원 이하의 과태료)
※ 다른 법령에 따라 보존하여야 하는 경우 보존 가능

- ▶ 개인정보 파기할 때에는 복구·재생되지 않도록 조치

- ▶ 다른 법령에 따라 보존하여야 하는 경우 다른 개인정보와 분리하여 저장·관리
(위반 시 1천만원 이하의 과태료)



파기 방법

- ▶ 기록물, 인쇄물, 서면, 기록매체
: 파쇄 또는 소각
- ▶ 전자적 파일 형태
: 복원이 불가능한 방법으로 영구 삭제

파기 절차

- ▶ 개인정보처리자
: 개인정보의 파기에 관한 사항을 기록 및 관리
- ▶ 개인정보 보호책임자
: 개인정보 파기 시행 후 파기 결과를 확인

3 개인정보의 처리



개인정보의 파기 (2)

01 파기 검토

보유기간 경과, 처리목적 달성된 경우 **지체 없이(5일 이내)** 파기
보존해야 하는 경우는 그 **법적 근거를 명확히** 확인(다른 개인정보와 **분리하여 저장·관리**)

02 파기 실시

복원 불가능한 방법으로 **완벽하게 파기**

구분	전자기적으로 기록된 개인정보	출력물 형태의 개인정보
종류	하드디스크, CD/DVD, USB 메모리 등	인쇄물, 서면 등
방법	재생시킬 수 없는 기술적 방법(디가우징 등) 또는 물리적 방법(천공기 등)으로 완전 파괴	파쇄 또는 소각하여 해당 개인정보를 완전 파기



03 기록·관리

개인정보의 파기 : 개인정보를 파기하고 내부결재 등을 통해 기록·관리

개인정보파일의 파기 : 개인정보파일 파기 관리대장에 기록·관리
[교육부 개인정보 보호지침 별지 제10호서식 사용]



04 결과 확인

개인정보 보호책임자(CPO)는 파기가 적절히 수행되었는지 **결과 확인**

보유목적을 달성한 개인정보의 **파기**는 법적 의무입니다.

[교육부]

3 개인정보의 처리



개인정보의 미파기 사례 (1)

침해
사례

» 요가강좌 운영사업자가 개인정보 파기를 요청한 이용자의 개인정보를 파기하지 않고
광고성 이메일 발송

10만원 손해배상 지급 결정 (분쟁조정위) (개인정보보호법 제21조 위반)



3 개인정보의 처리



개인정보의 미파기 사례 (2)

침해
사례

- 1년 이상 서비스에 접속하지 않은 이용자 정보를 파기하지 않은
7개 사업자 과징금 부과

과태료 500 ~ 1,000만원 (방통위) (정보통신망법 제29조 2항 위반)



1년이상
미접속



개인정보
미파기



4

개인정보의 침해 사례와 최신동향

4



가상화폐 거래소, 이메일 사용 부주의로 내부직원에 의한 개인정보 유출

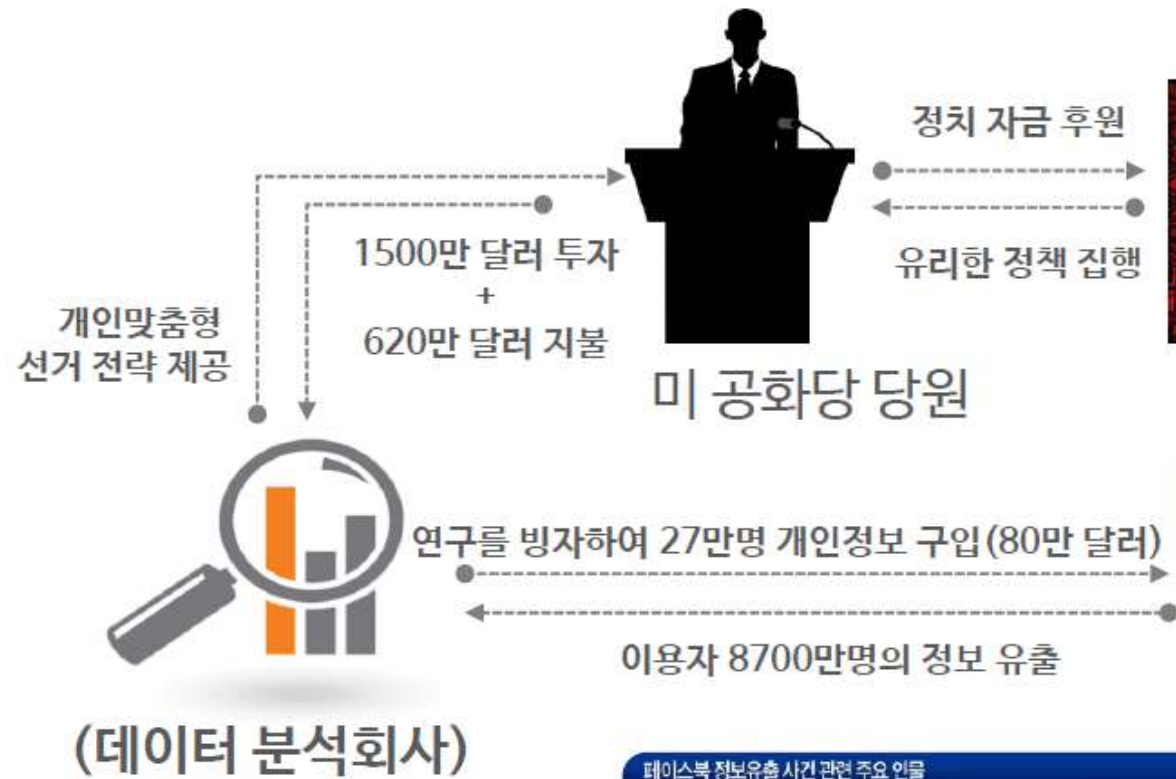
암호 화폐 명		수량	시세	환산 금액
비트코인 캐시	BCH	692	794,000	549,389,132
비트코인	BTC	2,016	6,893,000	13,897,264,824
엘프	ELF	409,962	570	233,678,129
이더리움	ETH	2,219	489,000	1,084,885,212
에토스	ETHOS	42,700	1,216	51,923,200
굴렘	GNT	1,015,090	335	340,055,150
에이치웨어	HSR	6,240	4,830	30,139,200
카이버 네트워크	KNC	50,000	837	41,850,000
오미세고	OMG	300	8,230	2,469,000
비체인	VEN	420	2,835	1,190,700
리플	XRP	5,227,490	519	2,713,067,310
합계				18,945,911,857

출처 : 더비체인 (<http://www.thebchain.co.kr>)

4 개인정보 침해사례 및 최신 동향



Facebook 개인정보 유출 파문



도널드 트럼프 대통령



페이스북 정보유출 사건 관련 주요 인물

고객정보 수집 및 활용, 정보 불법유출 사실 은폐	페이스북 고객정보 수집 및 불법 유출	페이스북 고객정보 가공해 트럼프 선거 지원	가공정보 선거에 활용
마크 저커버그 페이스북 CEO	알렉산더 코건 영국 케임브리지 대학교 교수	알렉산더 닉스 개입정보 기술 센터 (NSA) CEO	도널드 트럼프 미국 대통령

4 개인정보 침해사례 및 최신 동향



IoT기기 보안 취약으로 인한 유출 사고

- 유출내용 : **사생활 영상 등**
- 유출방법 : 관리자 계정 **설정이 취약한 IoT 기기**를 스캐닝, 접속, 악성코드 전파, 환경 설정이 미흡한 페이지를 접속하여 정보나 영상 탈취

신규 보안 취약점 신고포상제 연도별 운영 현황

시행 연도	전체		IoT	
	신고건수	포상건수	신고건수	포상건수
2012년	23	14	-	-
2013년	179	89	4	2
2014년	274	177	6	6
2015년	321	215	130	96
2016년	696	382	362	187
2017년	810	411	347	120
2018년	1,108	581	387	164
2019년 상반기	1,075	555	188	-
합 계	4,486	2,424	1,236	575

출처 : 한국인터넷진흥원(KISA) 2019.06

반려동물 사이트 및 IP카메라 해킹 개요도(A씨)



출처 : 2018.11 [한국일보]반려동물 사이트 및 IP카메라 해킹 개요도 그래픽=신동준 기자

4 개인정보 침해사례 및 최신 동향



개인정보 유출로 인한 기업의 피해

KBS NEWS

분야별 ▾

뉴스9 취재K 정보K 글로벌K 스포츠 **크립**

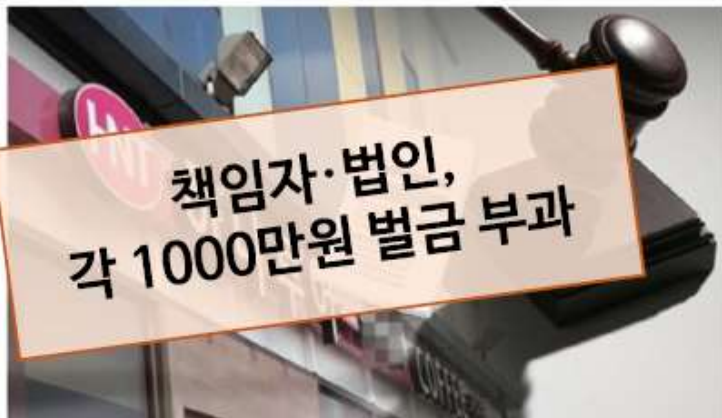
‘개인정보 49만 건 유출’ [redacted] 1심 벌금형 불복 항소

입력 2020.01.07 (18:16) | 수정 2020.01.07 (18:32)

사회

00 1 1 1 1

1 1 1 1



책임자·법인,
각 1000만원 벌금 부과

1심 판결 주요내용

**2017년 고객정보 유출 사고 → 과징금 처분
→ 검찰 불구속 기소 → 재판 → 1심 결과**

여권번호와 예약내역이 포함된 고객정보 유출
관리자가 별도의 인증 수단없이 아이디와 비밀번호만으로
고객정보가 담긴 시스템에 접근할 수 있었음
검찰증거를 종합해 볼 때 피고인(하나투어)의 유죄 인정 및
유출된 개인정보 규모나 유출경위 등을 고려해 형량 결정
(벌금형) 하나투어 법인과 정보보호 최고 책임자 김 모
본부장에게 각각 1천만원 선고

c.f. 2017년 9월 고객정보 유출 후 2018년 2월 과징금
3억 2725만원, 과태료 1800만원 부과

4 개인정보 침해사례 및 최신 동향

개인



정신적 피해뿐만 아니라 명예도용,
보이스피싱에 의한 금전적 손해,
유괴 등 각종 범죄에 노출

기업



기업의 이미지 실추 소비자단체
등의 불매운동, 다수 피해자에
대한 집단적손해배상시 기업
경영에 큰 타격

국가



프라이버시 라운드의 대두에 따른
IT산업의 수출애로, 전자정부의
신뢰성 하락, 국가 브랜드 하락

05

개인정보의 기술적 · 관리적 보호 조치

4 개인정보의 기술적·관리적 보호 조치

법적 근거

- ✓ 「개인정보보호법」 제29조 안전조치 의무
- ✓ 같은 법 시행령 제30조 제1항 (→참고)

목적

- ✓ 개인정보 분실·도난·유출·위조·변조·훼손되지 않게
기술적·관리적·물리적 안전조치의 최소 기준을 정함

적용 대상

- ✓ (자체 또는 타인을 통해) 개인정보를 처리*하는 모든 공공기관, 법인, 단체, 사업자, 개인 등
- * 업무를 목적으로 개인정보파일을 운용



4 개인정보의 기술적·관리적 보호 조치

[관련 법령 참고]

제23조(민감정보의 처리 제한)

- ② 개인정보처리자가 제1항 각 호에 따라 **민감정보**를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다.

제24조(고유식별정보의 처리 제한)

- ③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리 하는 경우에는 그 **고유식별정보**가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

제28조의4(가명정보에 대한 안전조치의무 등) 2020.8.5. 시행

- ① 개인정보처리자는 **가명정보**를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.
- ② 개인정보처리자는 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다.

※ 가명정보: 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정인을 알아볼 수 없는 정보 (개인정보보호법 제2조제1항 다목)

※ 추가정보: 개인정보의 전부 또는 일부를 대체하는 데 이용된 수단이나 방식(알고리즘 등) 가명정보와의 비교·대조 등을 통해 삭제 또는 대체된 개인정보 부분을 복원할 수 있는 정보
(매핑 테이블 정보 가명처리에 사용된 개인정보)

제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

4 개인정보의 기술적·관리적 보호 조치

[관련 법령 참고]

제21조(고유식별정보의 안전성 확보 조치) 법 제24조제3항에 따른 고유식별정보의 안전성 확보조치에 관하여는 제30조를 준용한다.

이 경우 “법 제29조”는 “법 제24조제3항”으로, “개인정보”는 “고유식별정보”로 본다.

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
5. 개인정보에 대한 보안프로그램의 설치 및 갱신
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

② 보호위원회는 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

제29조의5(가명정보에 대한 안전성 확보 조치)

① 개인정보처리자는 법 제28조의4제1항에 따라 가명정보 및 **가명정보**를 원래의 상태로 복원하기 위한 **추가 정보**(이하 이 조에서 “추가정보”라 한다)에 대하여 다음 각 호의 안전성 확보 조치를 해야 한다.

1. 제30조 또는 제48조의2에 따른 안전성 확보 조치

2. 가명정보와 추가정보의 분리 보관. 다만, 추가정보가 불필요한 경우에는 추가정보를 파기해야 한다.

3. 가명정보와 추가정보에 대한 접근 권한의 분리. 다만, 「소상공인 보호 및 지원에 관한 법률」 제2조에 따른 소상공인으로서 **가명정보**를 취급할 자를 추가로 둘 여력이 없는 경우 등 접근 권한의 분리가 어려운 정당한 사유가 있는 경우에는 업무 수행에 필요한 최소한의 접근 권한만 부여하고 접근 권한의 보유 현황을 기록으로 보관하는 등 접근 권한을 관리·통제해야 한다.

② 법 제28조의4제2항에서 “대통령령으로 정하는 사항”이란 다음 각 호의 사항을 말한다.

1. 가명정보 처리의 목적
2. 가명처리한 개인정보의 항목
3. 가명정보의 이용내역
4. 제3자 제공 시 제공받는 자
5. 그 밖에 가명정보의 처리 내용을 관리하기 위하여 보호위원회가 필요하다고 인정하여 고시하는 사항

4 개인정보의 기술적·관리적 보호 조치

안전성 확보 조치

✓ 안전성 확보에 필요한 기술적·관리적 및 물리적 조치

 1. 내부관리 계획의 수립 시행	 2. 접근권한의 관리	 3. 접근통제	 4. 개인정보의 암호화	 5. 접속기록의 보관 및 점검
 6. 악성 프로그램 등 방지	 7. 관리용 단말기의 안전조치	 8. 물리적 안전조치	 9. 재해·재난 대비 안전조치	 10. 개인정보의 파기

4 개인정보의 기술적·관리적 보호 조치

🔒 안전조치 미흡 → 개인정보 실태점검 위반 가장 큰 비중

(주요 위반항목) 개인정보 관리실태 현장점검



출처 : 행정안전부, 안전한 개인정보 관리를 위한 실태점검 길라잡이 15쪽

위반 내용별 행정 처분 현황

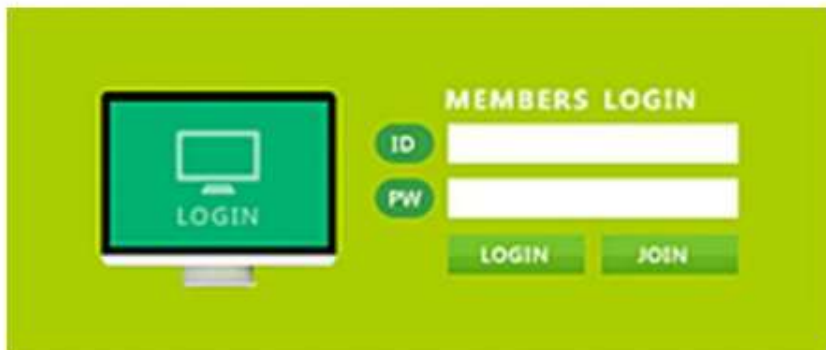
(단위 : 건)

구분	계	위반 내용별					
		안전조치 미흡	CCTV 관리 위반	미동의 / 과도 수집	동의 / 고지 방법 위반	위·수탁 관리 위반	방침 수립 등 기타
과태료	748	413	33	45	83	85	89
시정조치	661	104	156	65	112	100	124
개선권고	1,026	282	352	143	52	45	152
계	2,435	799	541	253	247	230	365
비율	100%	32.81%	22.22%	10.39%	10.14%	9.45%	14.99%

출처 : 행정안전부, KISA, 2013 ~ 2017 개인정보 실태 점검 및 행정 처분 사례집 2018, 39면

4 개인정보의 기술적·관리적 보호 조치

🔒 접근권한의 관리(제 5조)



“접근권한이란 개인정보처리시스템에 접속, 업무처리/개인정보 생성·변경·열람·삭제 권한

- ✓ 개인정보처리시스템에 대한 접근 권한은 **업무 수행에 필요한 최소한의 범위**로 업무 담당자에 따라 차등 부여
- ✓ 전보, 퇴직 등의 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 **접근 권한 변경 또는 말소**
- ✓ 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 최소 3년간 보관
- ✓ 개인정보처리시스템의 사용자계정 발급 시 **개인정보취급자 별로 발급**하며, 다른 취급자와 공유되지 않도록 함
- ✓ 안전한 비밀번호를 설정하여 이행할 수 있도록 **비밀번호 작성 규칙**을 수립하여 적용
- ✓ 계정정보 또는 비밀번호를 **일정 횟수 이상 잘못 입력한 경우** 접근 제한 등 필요한 기술적 조치

4 개인정보의 기술적·관리적 보호 조치

접근권한 관리 절차 사례



4 개인정보의 기술적·관리적 보호 조치

🔒 접근권한 관리 절차 사례

✓ 접근 권한 신청 (공문처리)

- 개인정보의 이용·활용 목적, 근거
- 개인정보의 이용·활용 업무의 범위



사용자 접근 권한 생성·변경 신청서

시스템명			
업무			
소속(부서)			
성명		사용자 ID	
사원번호		사용자 IP	
접근권한	개인정보 업무처리를 위해 필요한 접근권한 (생성, 열람, 정정, 삭제)을 작성함		
신청사유			

위와 같이 정보시스템 사용자 권한 생성(), 변경()을
신청합니다.

년 월 일
신청자 :

4 개인정보의 기술적·관리적 보호 조치

🔒 권한 없는 접근

- ✓ 우연히 알게 된 타인 ID/패스워드로 승낙없이 접속 (서울동부지법, 2003고단4200)
- ✓ 과거 직무상 알게 된 패스워드로 퇴직 후 접속 (서울지법, 2002고단9232)
- ✓ 동사무소 상근역, 직원 패스워드로 주민전산망 접속 (서울지법, 2002고단 12011)

🔒 양도받은 패스워드를 이용한 접속

A소령은 업무상 피고인인 최대위와 ID/PW를 공유



피고인은 A소령 ID/PW로 육군 웹메일 접속, 사령관에게 협박 메일



4 개인정보의 기술적·관리적 보호 조치

🔒 계정 공유 안전조치 의무위반 : 접속기록 점검으로 적발된 사례

✓ 동일IP에서 다수ID접속

- 하나의 업무PC에서 여러 계정을 공유하여 사용
- 친분이 있는 타부서의 업무를 도와주고자 계정을 공유하여 사용
- 계정이 부여되지 않은 공익요원과 계정을 공유하여 사용
- 업무보조자와 계정을 공유하여 사용



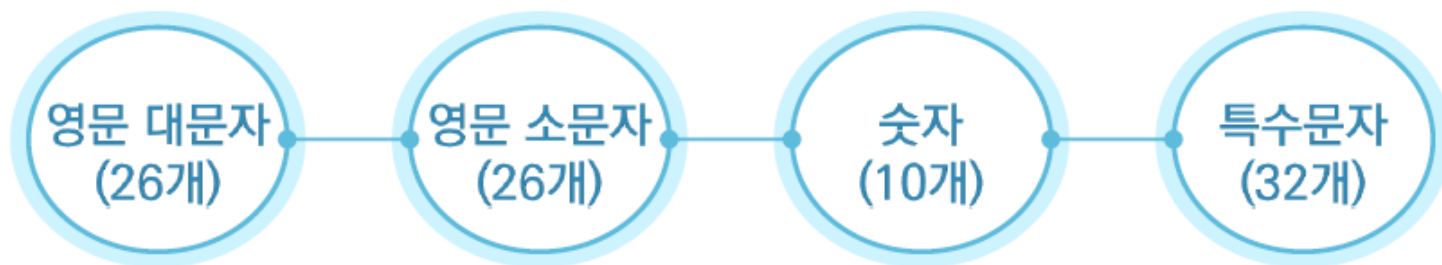
4 개인정보의 기술적·관리적 보호 조치



안전한 비밀번호 작성규칙 수립·이행

개인정보취급자를 대상으로 비밀번호 작성규칙을 수립하여 적용·운용

- 2종류 이상의 문자를 조합하여 최소 10자리 이상 또는 3종류 이상의 문자를 조합하여 최소 8자리 이상의 길이로 구성



- 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고
- 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경

4 개인정보의 기술적·관리적 보호 조치

물리적 안전조치(제11조)

제11조(물리적 안전조치)

- ② 개인정보처리자는 **개인정보가 포함된 서류, 보조저장매체 등을 잠금 장치가 있는 안전한 장소에 보관하여야 한다.**



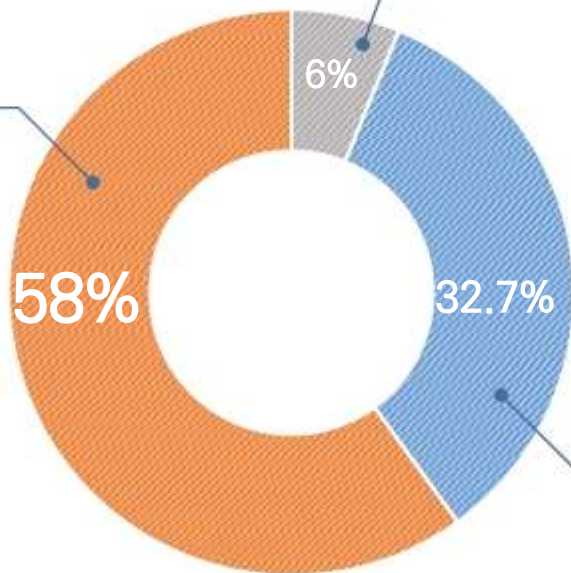
자료설명 : 개인정보가 포함된 서류, 보조저장매체 등을 책상위에 보관하고 있음

4 개인정보의 기술적·관리적 보호 조치

개인정보 유출사고 원인 Top 3

해킹

- 웹셀 업로드
- 파라미터 변조
- SQL인젝션 등 해킹공격



고의유출

- 퇴사 시 USB로 개인정보 다운로드
- 흥신소를 통한 개인정보 파일 구매
- 업무담당자가 지인에게 무단 제공



업무과실

- 담당자 실수로 인한 이메일 오발송
- 접근통제 미흡으로 구글 검색엔진 노출

4 개인정보의 기술적·관리적 보호 조치

게시글, 댓글 및 첨부파일 인한 개인정보 노출

노출사례(1)

- 관리자의 게시글 및 댓글로 인한 개인정보 노출

○ 신기술개발자

- 회사명 : [REDACTED]
- 대표자 : [REDACTED]
- 법인(주민)등록번호 : 110111 [REDACTED], 750505-[REDACTED]
- 주 소 : 서울시 송파구 [REDACTED], 서울시 강남구 [REDACTED]

○ 신기술 내용 및 범위

- [REDACTED] 공동접지기술

○ 신기술 보호기간 : 지정·고시일로부터 3년

다음글	[REDACTED] 전원개발사업실시계획(변경)
이전글	[REDACTED] 품질경영 및 공산품안전관리법 시행령 전부개정령

작성자 : 김 [REDACTED] 작성일 : 2018.06.29 방문 : 10
제목 : 외국인 등록번호로 회원가입

안녕하세요.

이번에 교환학생으로 재학중인 외국인 친구가 회원가입을 하려고 하는데, 아이폰, 휴대폰이 없어서 본인확인이 불가능해서 회원가입을 못하고 있습니다.

외국인 등록번호로 회원가입을 할 수 있다고 들었는데 어떻게 해야하나요?
자세한 사항은 통화로 말씀드리고 싶네요.

관리자님 글 확인하시면 전화좀 부탁드립니다.

[다음글] 다음글이 없습니다.
[이전글] 이전글이 없습니다.

목록 답변 수정 삭제

한줄답변

관리자 전화로 말씀하신 외국인 분의 이름 [REDACTED], 외국인등록번호 90 [REDACTED] (06.29) [REDACTED]가 맞나요? 빠른 시일내에 처리해드리겠습니다.

수정 삭제

4 개인정보의 기술적·관리적 보호 조치

엑셀 : Sheet[숨기기] 처리

노출 사례

- 숨겨진 시트에 있었던 개인정보가 노출되는 사례

The diagram illustrates a security vulnerability in Excel where hidden sheets can be accessed. It consists of three sequential screenshots:

- Initial State:** A spreadsheet titled "2020년 2학기" with columns for "학기", "성명", and "전공여부". A red circle highlights the "숨기기 취소" (Unhide) option in the context menu.
- Confirmation:** A dialog box titled "숨겨진 시트 확인" (Hidden Sheet Confirmation) appears, asking for confirmation to unhide the sheet. A red circle highlights the "확인" (Confirm) button.
- Result:** The hidden sheet is revealed, showing a table with personal information. A red box highlights the "주민등록번호" (Residential Registration Number) column, which contains masked data. An orange callout box points to this area, stating "숨겨진 시트에 있었던 개인정보" (Personal information that was in the hidden sheet).

Below the third screenshot, an orange callout box states: "숨겨져 있는 시트가 나타남" (Hidden sheet appears).

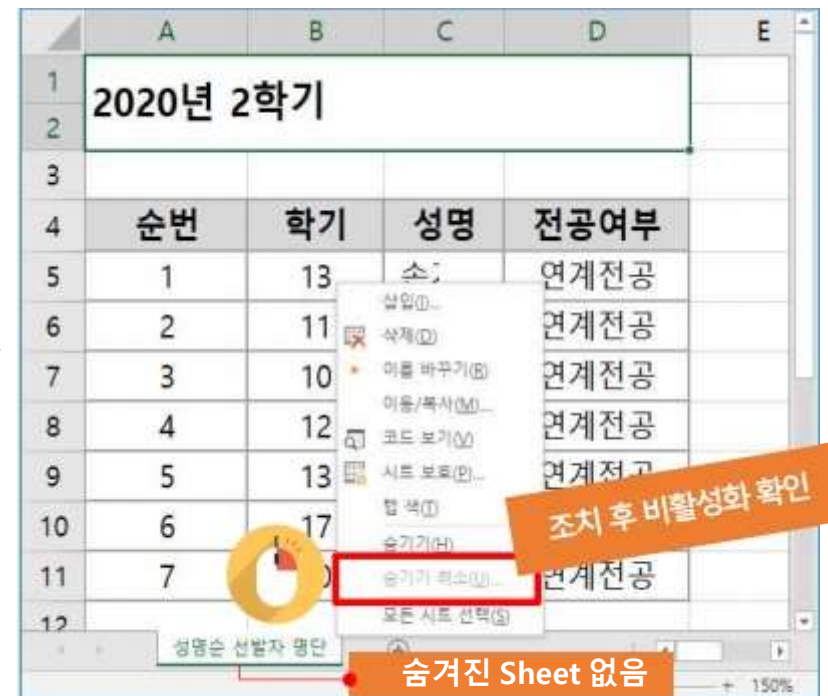
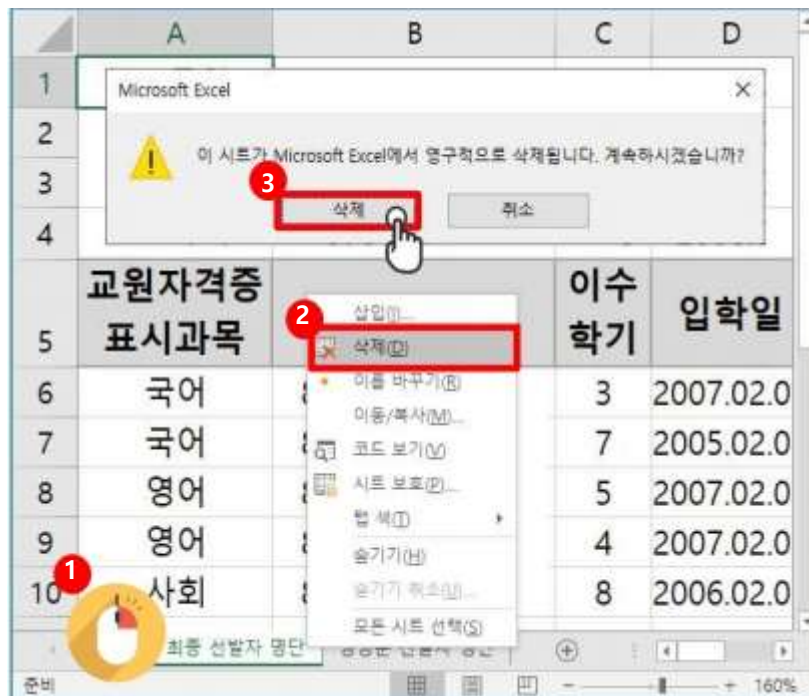
교원자격증 표시과목	주민등록번호	이수 학기	입학일
국어	881114- [Masked]	3	2007.02.0
국어	860901- [Masked]	7	2005.02.0
영어	880319- [Masked]	5	2007.02.0
영어	880306- [Masked]	4	2007.02.0
사회	870403- [Masked]	8	2006.02.0

4 개인정보의 기술적·관리적 보호 조치

엑셀 : Sheet[숨기기] 처리

조치방법

- 숨기기 처리된 Sheet 삭제 조치



4 개인정보의 기술적·관리적 보호 조치

엑셀 : 치환 함수

노출사례(1)

- 치환 함수 및 행/열 숨김으로 인한 노출사례

함수명	사용 함수	기존값	결과값
REPLACE	=REPLACE(A1,9,6,'*****')	801212-1234567	801212-1*****
SUBSTITUTE	=SUBSTITUTE(A1,'234567','*****')	801212-1234567	801212-1*****
LEFT	=LEFT(A1,8)&'*****'	801212-1234567	801212-1*****

텍스트의 일부를
다른 텍스트로 치환



A	B	C
1	801212-1234567	801212-1*****

텍스트 중의 old_text를 찾아서
원하는 new_text로 변경



A	B	C
1	801212-1234567	801212-1*****

텍스트 문자열의 시작지점부터
지정 한수만큼의 문자를 반환



A	B	C
1	801212-1234567	801212-1*****

4 개인정보의 기술적·관리적 보호 조치

엑셀 : 치환 함수

노출사례(2)

- 치환함수로 마스킹 처리된 필드를 해제/취소한 경우 노출

The image shows an Excel spreadsheet with a table of data. The formula bar at the top displays the formula `=REPLACE(15,9,6,"*****")`. A red arrow points from the formula bar to cell D5, which contains the masked phone number `440227-1*****`. An orange callout box with the text "15셀에 연결되어 있는 치환 함수" (Replacement function connected to cell 15) points to the formula bar. The table has columns for '판매소명' (Store Name), '주소' (Address), '대표자명' (Representative Name), and '주민등록번호' (Residential Registration Number). The data rows show various stores and their masked phone numbers.

	A	B	C	D
1	대형폐기물 스티커 판매 현황			
2				
3				
4	판매소명	주소	대표자명	주민등록번호
5	AA 마트	SS시 AA구 FA동	조가식	440227-1*****
6	BB 타운	SS시 ZZ구 EA동	조가숙	621013-2*****
7	NN 마트	SS시 AS구 AS동	김가숙	561230-2*****
8	HH 슈퍼	SS시 AW구 SS동	이가숙	550424-2*****
9	YY 철물	SS시 AZ구 QE동	이가호	780822-1*****
10	SS 슈퍼	SS시 AX구 EF동	조기자	630417-1*****
11	LL 마트	SS시 AS구 EB동	유가령	691110-2*****
12	AB 동점	SS시 AW구 QB동	남기훈	750126-1*****
13	BC 상회	SS시 BA구 CV동	김가자	741231-1*****
14	SF 슈퍼	SS시 WE구 RE동	이기태	640717-1*****
15	CZ 유통	SS시 CD구 VD동	이기창	590923-1*****
16	QW 슈퍼	SS시 WF구 ER동	오가용	870402-1*****
17	BD 점	SS시 GD구 EW동	김기수	750125-1*****
18	ASE 점	SS시 EZ구 WA동	광기수	660522-1*****

4 개인정보의 기술적·관리적 보호 조치

엑셀 : 치환 함수

조치방법

- 치환함수가 들어있는 행/열 복사 및 '값' 붙여넣기

D1 =REPLACE(D5,9,6,"*****")

판매소명	주소	대표자명	주민등록번호	주민등록번호
AA 마트	SS시 AA구 FA동	조가식	440227-1*	
BB 타운	SS시 ZZ구 EA동	조가숙	621013-2*	
NN 마트	SS시 AS구 AS동	김가숙	561230-2*	
HH 슈퍼	SS시 AW구 SS동	이가숙	551230-2*	
YY 칠물	SS시 AZ구 QE동	이가호	780123-1*	
SS 슈퍼	SS시 AX구 EF동	조기자	630417-1*	
LL 마트	SS시 AS구 EB동	유가령	691110-2*	
AB 동점	SS시 AW구 QB동	남기훈	750126-1*	
BC 상회	SS시 BA구 CV동	김가자	741231-1*	
SF 슈퍼	SS시 WE구 RE동	이기태	640717-1*	
CZ 유통	SS시 CD구 VD동	이기창	590923-1*	
QW 슈퍼	SS시 WF구 ER동	오가용	870402-1*	
BD 점	SS시 GD구 EW동	김기수	750125-1*	
ASE 점	SS시 EZ구 WA동	광기수	660522-1*	

1. 주민등록번호 셀 선택
2. 마우스 우클릭
3. '값' 붙여넣기 옵션 선택



D1 =440227-1*****

판매소명	주소	대표자명	주민등록번호	주민등록번호
AA 마트	SS시 AA구 FA동	조가식	440227-1*****	440227-1;
BB 타운	SS시 ZZ구 EA동	조가숙	621013-2*****	621013-2;
NN 마트	SS시 AS구 AS동	김가숙	561230-2*****	561230-2;
HH 슈퍼	SS시 AW구 SS동	이가숙	551230-2*****	
YY 칠물	SS시 AZ구 QE동	이가호	780123-1*****	
SS 슈퍼	SS시 AX구 EF동	조기자	630417-1*****	630417-1;
LL 마트	SS시 AS구 EB동	유가령	691110-2*****	691110-2;
AB 동점	SS시 AW구 QB동	남기훈	750126-1*****	750126-1;
BC 상회	SS시 BA구 CV동	김가자	741231-1*****	741231-1;
SF 슈퍼	SS시 WE구 RE동	이기태	640717-1*****	640717-1;
CZ 유통	SS시 CD구 VD동	이기창	590923-1*****	590923-1;
QW 슈퍼	SS시 WF구 ER동	오가용	870402-1*****	870402-1;
BD 점	SS시 GD구 EW동	김기수	750125-1*****	750125-1;
ASE 점	SS시 EZ구 WA동	광기수	660522-1*****	660522-1;

4. '값' 붙여넣기 옵션 선택
5. '값' 붙여넣기 옵션 선택
6. '값' 붙여넣기 옵션 선택

4 개인정보의 기술적·관리적 보호 조치

엑셀 : 치환 함수

조치방법

- 원본 행/열 삭제 및 연결된 값 확인

Excel screenshot showing the initial state of a spreadsheet. The formula bar shows '=440227-1*****'. The spreadsheet has columns A through I. Row 4 is the header row. Rows 5-18 contain data. A red box highlights the formula bar. A red box highlights the cell D1. A red box highlights the cell D18. A red box highlights the cell D18. A red box highlights the cell D18.

판매소명	주소	대표자명	주민등록번호
AA 마트	SS시 AA구 FA동	조가식	440227-1*****
BB 타운	SS시 ZZ구 EA동	조가숙	621013-2*****
NN 마트	SS시 AS구 AS동	김가숙	561230-2*****
HH 슈퍼	SS시 AW구 SS동	이가숙	550424-2*****
YY 칠물	SS시 AZ구 QE동	이가호	780822-1*****
SS 슈퍼	SS시 AX구 EF동	조기자	630417-1*****
LL 마트	SS시 AS구 EB동	유가령	691110-2*****
AB 동점	SS시 AW구 QB동	남기훈	750126-1*****
BC 상회	SS시 BA구 CV동	김가자	741231-1*****
SF 슈퍼	SS시 WE구 RE동	이기태	640717-1*****
CZ 유통	SS시 CD구 VD동	이기창	590923-1*****
QW 슈퍼	SS시 WF구 ER동	오가용	870402-1*****
BD 점	SS시 GD구 EW동	김기수	750125-1*****
ASE 점	SS시 EZ구 WA동	광기수	660522-1*****



Excel screenshot showing the result of the deletion process. The formula bar shows '=440227-1*****'. The spreadsheet has columns A through D. Row 4 is the header row. Rows 5-18 contain data. A red box highlights the formula bar. A red box highlights the cell D1. A red box highlights the cell D18. A red box highlights the cell D18. A red box highlights the cell D18.

판매소명	주소	대표자명	주민등록번호
AA 마트	SS시 AA구 FA동	조가식	440227-1*****
BB 타운	SS시 ZZ구 EA동	조가숙	621013-2*****
NN 마트	SS시 AS구 AS동	김가숙	561230-2*****
HH 슈퍼	SS시 AW구 SS동	이가숙	550424-2*****
YY 칠물	SS시 AZ구 QE동	이가호	780822-1*****
SS 슈퍼	SS시 AX구 EF동	조기자	630417-1*****
LL 마트	SS시 AS구 EB동	유가령	691110-2*****
AB 동점	SS시 AW구 QB동	남기훈	750126-1*****
BC 상회	SS시 BA구 CV동	김가자	741231-1*****
SF 슈퍼	SS시 WE구 RE동	이기태	640717-1*****
CZ 유통	SS시 CD구 VD동	이기창	590923-1*****
QW 슈퍼	SS시 WF구 ER동	오가용	870402-1*****
BD 점	SS시 GD구 EW동	김기수	750125-1*****
ASE 점	SS시 EZ구 WA동	광기수	660522-1*****

연결된 값이 없는지 확인

4 개인정보의 기술적·관리적 보호 조치



개인정보 유출신고 방법

관련 규정

- ✓ 개인정보가 유출되었음을 인지한 때에는 지체 없이 해당 정보주체에게 통지
- ✓ 피해 최소화를 위한 대책 마련 및 조치, 개인정보보호위원회/KISA에 신고 필요

*** 개인정보처리자 : 5일 이내 통지, 1천건 이상 신고 / 정보통신제공자 : 24시간 이내 통지 및 신고**

01

유출된 정보주체 개개인에게 지체없이 통지
(개인정보 보호법 제34조 제1항)

시한

유출되었음을 알게 되었을 경우 지체없이(5일 이내)

통지항목

- ① 유출된 개인정보의 항목
- ② 유출 시점과 그 경위
- ③ 피해 최소화를 위한 정보주체의 조치방법
- ④ 기관의 대응 조치 및 피해 구제 절차
- ⑤ 피해 신고 접수 담당부서 및 연락처

02

피해 최소화를 위한 대책 마련 및 필요한 조치 실시
(개인정보 보호법 제34조 제1항)

- 접속 경로 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 피해를 최소화하기 위해 필요한 긴급조치 이행
- 긴급 조치 이행 등에 어려움이 있는 경우 전문기관에 기술 지원 요청

* 피해 최소화 대책을 마련하지 않거나 필요한 긴급 조치를 하지 않은 경우:
시정명령

4 개인정보의 기술적·관리적 보호 조치

관련 규정

- ✓ 개인정보가 유출되었음을 인지한 때에는 지체 없이 해당 정보주체에게 통지
- ✓ 피해 최소화를 위한 대책 마련 및 조치, 개인정보보호위원회/KISA에 신고 필요

* 개인정보처리자 : 5일 이내 통지, 1천건 이상 신고 / 정보통신제공자 : 24시간 이내 통지 및 신고

03

1천 명 이상 유출된 경우 유출 통지 결과 신고
(개인정보 보호법 제34조 제3항)

- 1천명 이상 유출된 경우 유출 통지 및 조치 결과를 지체 없이 개인정보보호위원회 또는 전문기관 (한국인터넷진흥원)에 신고

* 개인정보보호법 제75조제2항제9호(3천만 원 이하의 과태료) 조치 결과를 신고하지 않은 자(개인정보보호위원회 또는 전문기관에 통지 결과 등을 신고하지 않은 경우)

04

1천 명 이상 유출된 경우에는 추가로 홈페이지에 공지
(개인정보 보호법 시행령 제40조 제3항)

- 1천명 이상 개인정보가 유출된 경우 개별 통지와 함께 유출된 사실을 인터넷 홈페이지에 7일 이상 게재

* 홈페이지 등에 공지하지 않거나 7일 미만으로 게재하는 경우:시정명령

4 개인정보의 기술적·관리적 보호 조치



개인정보 유출신고 방법

개인정보 유출 신고 절차

1 개인정보보호 포털(www.privacy.go.kr) 접속

2 민원마당 내 '개인정보 유출·침해신고' 클릭

3 대상 선택 후 '신고하기' 클릭

4 유출신고 작성예시

4 개인정보의 기술적·관리적 보호 조치



개인정보 유출신고 방법

개인정보 유출통지 의무

✓ (개인정보보호법 제34조 제1항)

|시한| 유출되었음을 알게 되었을 경우 지체 없이 통지(통상 5일 이내)

통지항목

- ① 유출된 개인정보의 항목
- ② 유출 시점과 그 경위
- ③ 피해 최소화를 위한 정보주체의 조치방법
- ④ 기관의 대응 조치 및 피해 구제 절차
- ⑤ 피해 신고 접수 담당부서 및 연락처

통지방법

- ① 통지는 서면 등의 방법으로 하여야 함
- ② 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법을 이용한 개별적 통지 방법이면 가능
- ③ 확인사실의 우선통지 (유출된 개인정보의 항목, 유출 시점 및 그 경위의 구체적인 내용을 확인하지 못한 경우 → 추후 확인되는 사항을 추가로 알릴 수 있음)
- ④ 개인정보가 유출되었음을 알게 되었을 때 통지 의무가 발생, 유출사실을 개인정보처리자가 인지한 시점에서 유출통지 의무가 발생

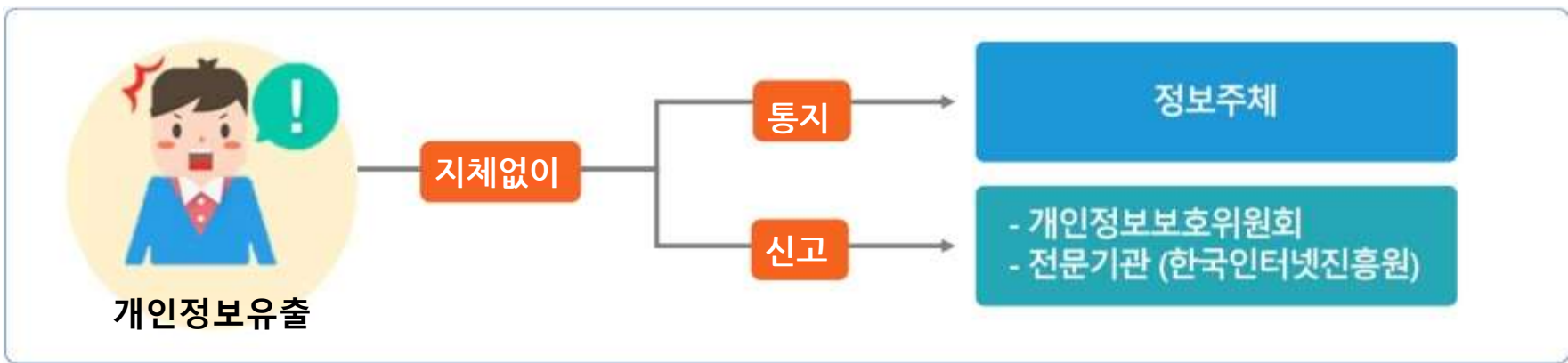


4 개인정보의 기술적·관리적 보호 조치



개인정보 유출통지 방법

유출통지 방법



통지방법	
통지대상	1건이라도 개인정보 유출 시, 정보주체에게 유출관련 사실을 통지
통지시기	5일 이내(개인정보보호법), 24시간 이내(정보통신망법)
통지방법	개별 통지 - 서면, 전자우편, 전화, 팩스, 문자전송 등 ※ 1천명 이상의 개인정보가 유출된 경우, 서면 등의 방법과 함께 인터넷 홈페이지에 7일 이상 게재 (개인정보보호법)
통지내용	유출된 개인정보의 항목, 유출된 시점과 그 경위, 정보주체의 피해 최소화 방법, 사업자의 대응조치 및 피해구제 절차, 담당부서 및 연락처

4 개인정보의 기술적·관리적 보호 조치



개인정보 유출통지 방법



개인정보 유출 통지 사례

○○를 믿고 아껴 주시는 회원 여러분

그동안 ○○은 회원님의 개인정보 보호를 위해 최우선으로 노력하여 왔으나, 불의의 사고로 회원님의 소중한 개인정보가 유출되었음을 알려드리며, 이에 대하여 진심으로 사과를 드립니다.

(① 유출 시점과 그 경위)

3월초, 서울 경찰청 사이버수사대에서 개인정보 유출과 관련하여 관리실태를 점검 중에 유출 정황 발견됐으며 이후 내부 개발팀의 진단 결과, 회원님의 개인정보는 2018년 4월 1일 14시 40분경 해커에 의한 해킹으로 유출 된 것으로 밝혀졌습니다.

(② 유출된 개인정보의 항목)

유출된 개인정보 항목은 아이디(ID)와 이메일, 집 전화번호, 휴대폰번호, 생년월일 총 5개 입니다.

다행히, 개정된 정보통신망법에 따라 주민등록번호는 전량 폐기 후 수집하지 않고 있으며, 비밀번호도 암호화로 보호돼 유출되지 않은 것으로 확인되었습니다.

(③ 기관의 대응 조치)

○○는 유출 사실을 인지한 후 즉시 취약점 점검과 보완조치를 하였습니다. 한편, 전화번호 및 휴대폰번호는 개인정보암호화 작업으로 보안을 강화하였으며 웹 방화벽, IPS 장비를 이용해 현재도 강력한 보완유지에 힘쓰고있습니다.

4 개인정보의 기술적·관리적 보호 조치



개인정보 유출통지 방법



개인정보 유출 통지 사례

(④ 피해 최소화를 위한 정보주체의 조치방법)

비밀번호는 유출되지 않았지만 혹시 발생할지 모를 타 웹사이트에서의 2차 피해를 방지하기 위하여 번거로우시더라도 고객님의께서는 현재 사용하시는 비밀번호를 변경하여 주시기 바랍니다. 또한 웹사이트에서 사용하고 계시는 동일한 아이디나 비밀번호의 경우, 해당 웹사이트에 방문하셔서 비밀번호를 변경하시는 것이 안전함을 알려 드립니다.

(⑤ 피해 구제 절차)

아울러 피해가 발생하거나 예상되는 경우에는 아래 담당부서에 신고하시면 성실하게 안내와 상담을 해드리겠습니다.

앞으로 장애처리 과정에 대한 개인정보 보호 조치 강화 등 내부 개인정보 보호 관리체계를 개선하고, 관계 직원 교육을 통해 인식을 제고하여, 향후 다시는 이와 유사한 사례가 발생하지 않도록 최선의 노력을 다하겠습니다. 뜻하지 않게 개인 정보가 유출되어 회원 여러분의 심려를 끼쳐드린 점에 대해 거듭 진심으로 사과 드립니다.

(⑥ 피해 신고 접수 담당부서 및 연락처)

- 피해 등 접수 담당부서: ○○ 운영팀
- 피해 등 접수 전화번호: 02-2164-1004
- 피해 등 접수 E-메일주소: ANGEL@GOD.COM

4 개인정보의 기술적·관리적 보호 조치



개인정보 유출통지 방법



개인정보 처리자 A

연락가능한 개인정보 항목 1. 핸드폰 번호
2. 이메일 주소

1차 유출 통지: 이메일주소를 통해 메일 발송
(10만 명 중 4만 건은 반송)

2차 유출 통지: 휴대폰 번호를 통해 SMS 발송
(4만 명 중 2만 건은 반송)

개인정보 처리자 B

연락가능한 개인정보 항목 1. 핸드폰 번호
2. 이메일 주소
3. 집주소

1차 유출 통지: 이메일주소를 통해 메일 발송
(10만 명 중 4만 건은 반송)

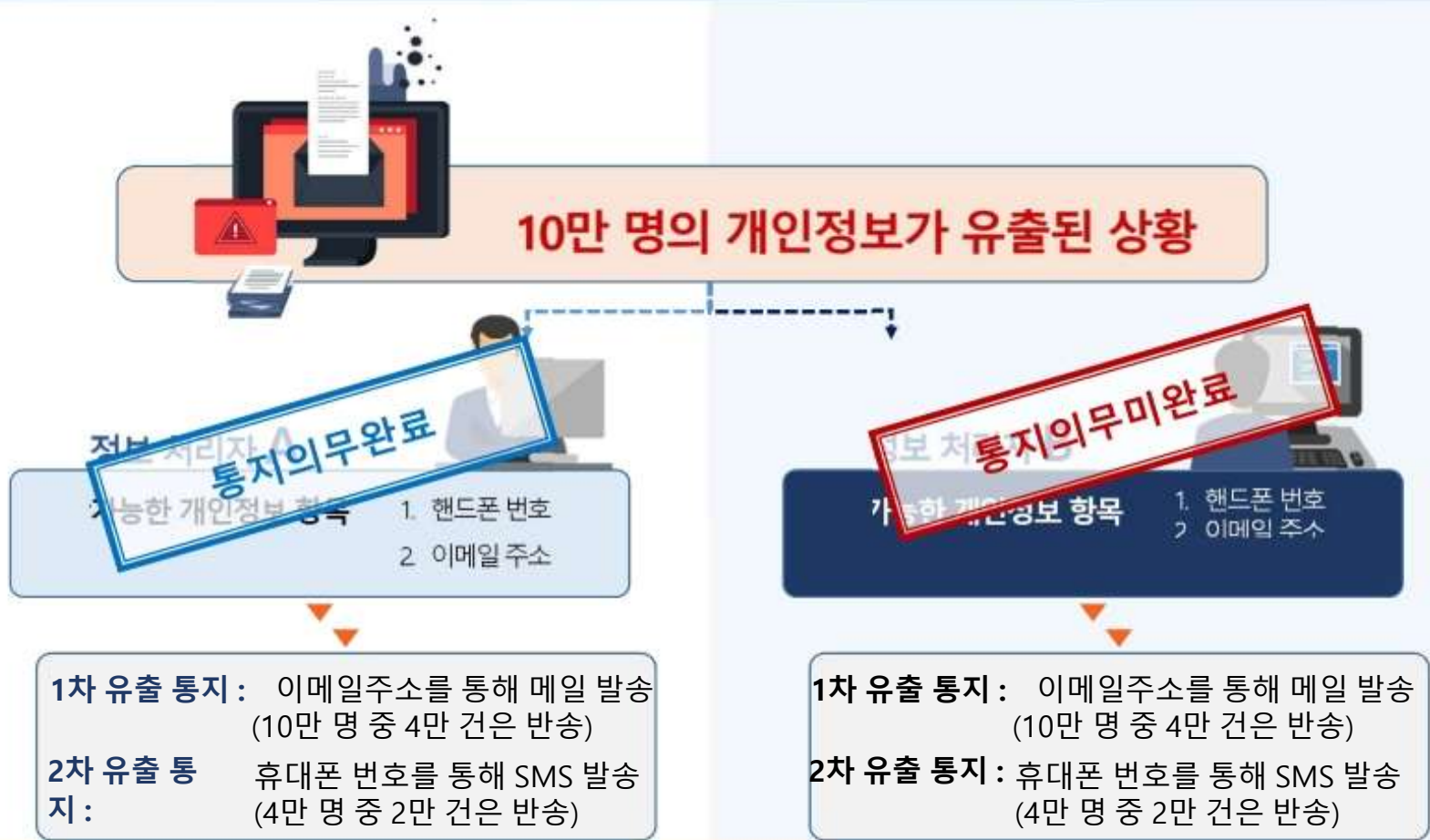
2차 유출 통지: 휴대폰 번호를 통해 SMS 발송
(4만 명 중 2만 건은 반송)

Q 두 사람 중 유출 통지의무를 다하지 않은 사람은?

4 개인정보의 기술적·관리적 보호 조치



개인정보 유출통지 방법



A는 유출 통지 의무를 완료했다고 보여지나,
B는 2만 명에 대해 유출통지하지 않았음 (집주소를 가지고 있었음에도 불구하고)

4 개인정보의 기술적·관리적 보호 조치



개인정보 유출사고 조치 및 책임

행정처분 흐름도



- 개인정보보호법



- 개인정보보호위원회의 현장조사(KISA)



- 과태료, 과징금
- 영업정지(취소), 임원/기관 징계

4 개인정보의 기술적·관리적 보호 조치



개인정보 유출사고 조치 및 책임



민사

✓ 제39조의 2 (법정손해배상의 청구)

- ① 제39조제1항에도 불구하고 정보주체는 개인정보처리자의 고의 또는 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 **300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다.** 이 경우 해당 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.
- ② 법원은 제1항에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를 고려하여 제1항의 범위에서 상당한 손해액을 인정할 수 있다.
- ③ 제39조에 따라 손해배상을 청구한 정보주체는 사실심(事實審)의 변론이 종결되기 전까지 그 청구를 제1항에 따른 청구로 변경할 수 있다.

[본조신설 2015. 7. 24.]



4 개인정보의 기술적·관리적 보호 조치



개인정보 유출사고 조치 및 책임

행정벌

✓ 고시의 보호조치 **의무 위반과 유출사이의 인과관계를 요구하지 않음**(다만 '관련성'은 요구됨)

개인정보보호법 제34조의 2

(제1항)

보호위원회는 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 5억원 이하의 과징금을 부과·징수할 수 있다.

다만, 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보처리자가 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

개인정보보호법 제39조의 15

(제1항)

보호위원회는 정보통신서비스 제공자등에게 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자 등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.

(제1항 제5호)

이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우로서 제29조의 조치를 하지 아니한 경우

개인정보 보호조치

4 개인정보의 기술적·관리적 보호 조치



개인정보 유출사고 조치 및 책임

형사벌

✓ 제73조(벌칙)

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 **2년 이하의 징역 또는 2천만원 이하의 벌금**에 처한다. <개정 2015. 7. 24., 2016. 3. 29., 2020 2. 4..>

1. 제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 **안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자**
- 1의2. 제21조제1항을 위반하여 개인정보를 파기하지 아니한 정보통신서비스 제공자등
2. 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자
3. 제37조제2항을 위반하여 개인정보의 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 자



06

사이버 공격과 정보보안 수칙

개인정보 보호 생활규칙

■ 공공기관장, CPO 등은 개인정보보호 마인드 제고가 필요합니다!

- 개인정보보호 업무가 내부 **사업 중요도**에서 **후순위**로 밀리는 사례 다수 발견
- **보직자**의 개인정보에 대한 중요성을 인식하고 많은 관심과 **적극적인 지원 필요**



2 안전한 개인정보 보관·관리를 위해 적극적인 투자를 해주세요!

- 정보보호시스템* 등 투자 부족으로 '**개인정보 안전성 확보조치 기준**' 위반사항 **다수** 발견
* 침입차단시스템, 침입탐지시스템, 침입방지시스템, 웹방화벽, DB접근제어시스템, DB암호화솔루션 등
- 공통시스템(예:서울행정)에 비해 **자체 개발·도입 시스템이 취약**
- 특히 **노후화된 시스템**의 법규 준수여부를 체크 필요
- 적정 예산 확보를 통한 **지속적인 투자** 당부



개인정보 보호 생활규칙

■ 개인정보보호 전담인력을 배치·교육하고 전문성을 높여주세요!

- 전담인력이 없거나 전담인력의 잦은 교체로 업무 연속성 미흡 사례 빈번
- 개인정보파일 현황 파악 미흡, 내부관리계획 등 규정 정비 미흡 등 발견
- 보안 전문교육 등을 통해 개인정보보호 및 정보보호 인력의 안정적인 운영 필요



4 개인정보 유출사고의 주요 원인인 해킹방어에 힘써주세요!

- 사용 중인 OS 등 소프트웨어에 대한 최신 보안 업데이트 상시 적용(랜섬웨어)
- 홈페이지 개발 시 시큐어코딩 사용, 개발된 홈페이지의 경우 주기적인 웹취약점 분석
- 방화벽 등 보안장비의 보안정책을 주기적으로 점검 및 최신 이슈사항 반영
- 송신자가 명확하지 않은 메일 열람 금지, 블로그 등에서 받은 프로그램 실행 금지



개인정보 보호 생활규칙

■ 개인정보가 유출되었을 때는 정보주체에게 알려주세요!

- 유출된 정보주체 개개인에게 **지체없이**(5일 이내) **통지**(유출 항목/시점/경위, 대응방안)
- 1만명 이상 유출된 경우에는 **유출통지** 결과를 행안부/**KISA**에 신고하고 **홈페이지**에 **공지**
- 피해 최소화를 위한 대책 마련 및 필요한 조치 실시(유출된 개인정보의 삭제 등)



6 법령 및 고시 재·개정 사항을 지속적으로 모니터링 해주세요!

- '16.9. 시행된 '일정시간 미작동시 로그아웃', '비밀번호 오류 계정잠금' 등 미조치 다수
- 언론 등을 통해 법령 및 고시 **재·개정** 사항을 **파악**하고 법적 요구사항을 반영



Q&A

감사합니다