

취급단계별 개인정보보호 조치 사항

2010년 4월



행정안전부



한국인터넷진흥원

목 차

- 1 사업자가 생각해봐야 할 점
- 2 개인정보 취급단계별 원칙과 사례
- 3 관리적.기술적 보호조치
- 4 개인정보보호법 시행으로 바뀌는 점

1 사업자가 생각해봐야 할 점

1. 사업자가 생각해 봐야 할 점

우리 사업장에서 생각하여야 할 문제들

어떤 법 적용을 받는가 ?

사업 유형에 따라 적용되는
법률이 달라지므로
자신의 사업 유형에 따른
적용법률을 정확히 숙지해야 함

어떤 의무를 지켜야 하나 ?

개인정보의 취급 단계별로
다양한 원칙과 의무가 규정되어
있으므로 각각의 법적 의무를
잘 알아두어야 함

의무를 지키지 않으면 ?

- ① 의무사항 위반시 시정명령 및 과태료 등의 **행정처분** 부과
- ② 형사벌 규정 위반시 **형사처벌**
- ③ 이용자들로부터 **민사소송**

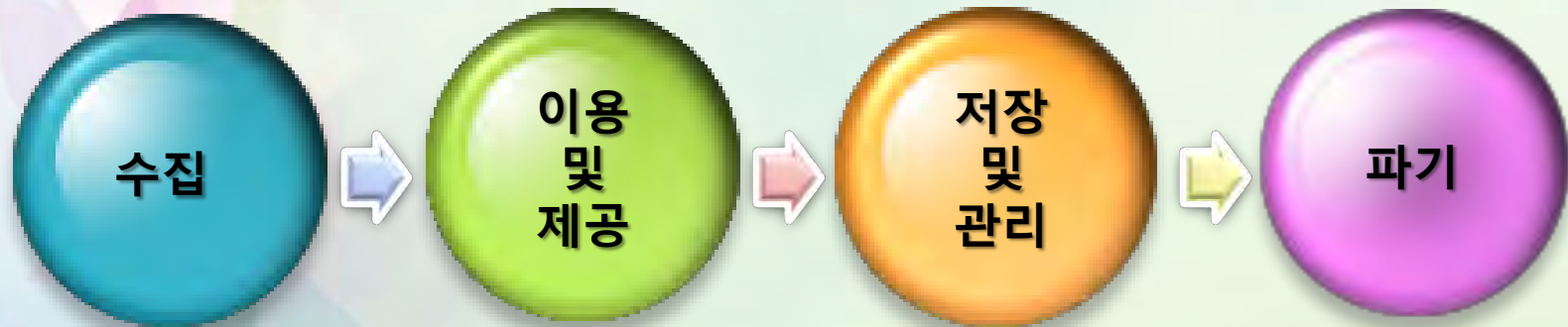
도움을 얻을 곳은?

- ① 행안부, KISA (118상담센터)
- ② 정부 주관 전문, 순회교육
- ③ 정부의 서면, 현장 실태점검
- ④ **개인정보보호 실천협의회** 등
사업자 자율협의체 가입 활동
(www.ppc21.or.kr)



1. 사업자가 생각해 봐야 할 점은?

개인정보 주기 (Life Cycle)에 따른 보호조치



관리적 보호조치

기술적 보호조치

물리적 보호조치

준용사업자와 정보통신망법

- 정보통신망법은 당초 **정보통신서비스 제공 사업자**에게 적용하기 위하여 제정된 법률
 - 인터넷이나 정보통신망을 통해 개인정보를 수집, 취급하는데 특화
 - 주로 오프라인에서 거래가 이루어지는 '**준용사업자**'에 대해서는 정보통신망법의 해석이 어려운 측면이 있음
- 서비스의 형태, 개인정보의 수집, 취급행태를 면밀히 고려하여 정보통신망법의 해석과 적용을 하여야 함

1. 사업자가 생각해 봐야 할 점은?

공공과 민간의 개인정보보호 차이점

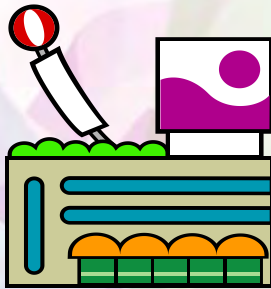
	공공	민간
수집	법률 규정에 의한 수집 공익 목적의 수집	서비스 제공을 위해 계약을 맺고 동의를 얻어 개인정보 수집
보호목적	국가 권력으로부터 국민의 인권 및 사생활 보호	사업자의 무분별한 개인정보 이용행위를 규제
피해구제	행정구제 절차	분쟁조정 및 사법구제(소송)

2 개인정보 취급단계별 원칙과 사례

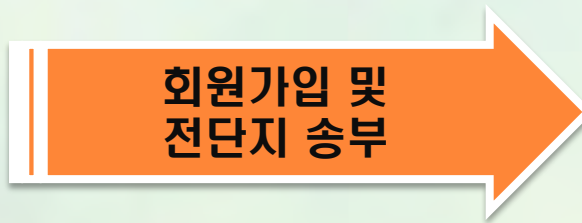
개인정보를 수집할 때는

	주요 내용
관련조항	정보통신망법 제22조
동의원칙	사업자는 이용자의 개인정보를 이용하기 위해 수집하는 경우 아래 고지사항을 알리고 동의 를 얻어야 함
수집시 고지사항	① 개인정보의 수집 · 이용 목적 ② 수집하는 개인정보의 항목 ③ 개인정보의 보유 및 이용 기간
예외	동의 없이도 개인정보 수집 가능한 경우 ? ① 계약 이행을 위해 필요한 경우로서 동의 취득이 곤란한 경우 ② 요금정산을 위해 필요한 경우 ③ 다른 법률에 특별한 규정이 있는 경우
벌칙	▪ 5년 이하 징역 또는 5천만원 이하 벌금

개인정보 수집 동의 미취득 사례



A 백화점



B씨

입점업체 직원에게
백화점 회원카드
모집 할당



실적 채워야 하니까
우선 가져다 쓰자
ㅎㅎㅎ

과거 근무했던 의류업체 고객시스템에서
동의없이 B씨 정보를 수집하여
백화점 회원에 가입시킴

생각해 볼 점

● 개인정보 수집에 대한 “동의”의 의미

- 개인정보를 “이용하기 위해 수집”하는 행위에 대해 동의받는 것이므로
- “수집, 이용목적”을 알리는 것이 필요하게 됨

● 준용사업자는 영업의 성격상, 동의받는 절차를 마련하기가 어렵다는 문제가 있음

- 예) 학원, 주택관리업, 부동산, 주유소 등

● 의료기관의 경우 개인정보 수집의 특이성이 존재함

- 예) 긴급환자, 의식불명인 환자에게 동의받을 수 있는지 여부

2. 민감정보, 최소정보 원칙

수집

이용 및
제공

저장 및
관리

파기

민감 개인정보, 최소 개인정보

민감 개인정보 수집

관련조항

정보통신망법 제23조 제1항

수집원칙

권리 · 이익 · 사생활을 현저하게
침해할 우려가 있는 정보는
원칙적으로 수집 금지
(사상, 신념, 병력 등의 정보)

특이사항

민감정보 수집의 예외

- ① 이용자의 명시적인 동의를 받은 경우
- ② 다른 법률에 따라 특별히 수집대상
개인정보로 허용된 경우

벌칙조항

- 5년 이하 징역 또는
5천만원 이하 벌금

최소 개인정보 수집

정보통신망법 제23조 제2항

서비스 제공에 필요한
최소한의 개인정보를 수집

필요 최소한의 정보를 제공하지
않는다는 이유로
서비스 제공을 거부할 수 없음

서비스 제공을 거부한 경우
3천만원 이하의 과태료

최소 개인정보 수집 위반 사례

A 씨

제 신용카드
이번달 금액이..?

신용카드 관련 문의로
전화상담

X 신용카드 회사
상담원



회원이 아니더라도
주민등록번호를 요청



네..고객님
주민등록번호가...

생각해 볼 점

- 민감정보와 최소정보는 절대적 개념이 아님
 - 준용사업자의 서비스 특성, 현황에 따라 달라지는 **상대적 개념**

예) 결혼중개업의 민감, 최소정보와

일반적인 인터넷 사업자의 민감, 최소정보는 매우 다를 수 있음

3. 아동의 개인정보 수집

수집

이용 및
제공

저장 및
관리

파기

아동의 개인정보를 수집해야 하는데

주요내용

관련조항

정보통신망법 제31조

원칙

사업자가 **만 14세 미만 아동**의 개인정보를 수집하거나
이용, 제공하려 하는 경우에는
법정대리인(부모)의 동의를 얻어야 함

벌칙조항

- 5년 이하 징역 또는 5천만원 이하 벌금

아동의 개인정보 수집 위반 사례



동의받은 목적 외로 이용할 수 없습니다

	내용
관련조항	정보통신망법 제24조
주요내용	준용사업자는 이용자로부터 동의받은 목적 과 다른 목적으로 개인정보를 이용할 수 없음
예외조항	▪ 이용자의 동의가 있는 경우 • 계약 이행을 위해 필요한 경우로서 동의 취득이 곤란한 경우 • 요금정산을 위해 필요한 경우 • 다른 법률에 특별한 규정이 있는 경우
벌칙조항	▪ 5년 이하 징역 또는 5천만원 이하 벌금

목적 외 이용 위반 사례 (1)



A씨 (보험고객)

보험서비스 가입

사전에 고지한 바 없는
별도의 보험 대출상품 마케팅



X 보험회사

사전에 동의받은 바 없는 별도의 상품 마케팅은
고객의 개인정보를 목적 외로 이용한 것이라고 법원 판결

목적 외 이용 위반 사례 (2)



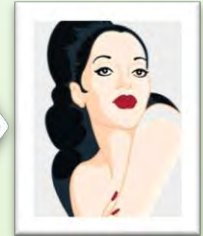
I'm happy

여대생 A양



얼굴 성형수술 시술

수술 전후사진
이용에 대해서
동의한 바 없음



수술 전후 얼굴사진을
홍보용으로 웹사이트 게재

생각해 볼 점

- 개인정보의 목적외 이용 금지 규정은 준용사업자가 사업 과정에서 가장 주의하여야 하는 규정임
 - “우리 고객이니까 괜찮겠지”라는 마음이 법률 위반의 계기가 됨
- 사회 통념상 사업에 필수적인 행위에 대해서는 개인정보 수집시 “수집, 이용목적”에 미리 반영하는 것이 필요
 - 해당 사업에 반드시 따르는 홍보, 마케팅 등
- 최근 법원, 정부는 이용자 권익 보호를 위하여 개인정보의 목적외 이용을 엄격하게 적용, 해석하는 경향

동의없이 제3자에게 제공할 수 없습니다

	내용
관련조항	정보통신망법 제24조의 2
주요내용	준용사업자는 개인정보를 제3자에게 제공하려면 아래의 고지사항을 이용자에게 알리고 동의 를 얻어야 함
고지사항	▪ 개인정보를 제공받는 자 ▪ 제공받는 자의 이용목적 ▪ 제공하는 개인정보 항목 ▪ 제공받는 자의 보유 및 이용 기간
예외사항	▪ 요금정산을 위해 필요한 경우 ▪ 다른 법률에 특별한 규정이 있는 경우
벌칙조항	▪ 5년 이하 징역 또는 5천만원 이하 벌금

제3자 제공 위반사례

Y 마트고객



Y 대형마트에서 물품 구입
후 받은 응모권으로
경품행사 참여

Y 대형마트



동의 없이
개인정보
제공



Z 생명보험사로부터
예금상품 TM 수신



Z 생명보험

개인정보 취급 업무를 위탁할 경우

필수 위탁

관련조항

정보통신망법 제25조 제2항

주요내용

서비스 제공 계약을 이행하기 위해
위해 필요한 개인정보 취급 위탁은
이용자에게 아래 사항을 고지
1 취급위탁을 받는 자 (수탁자)
2 취급위탁 업무 내용

예시

제품, 서비스 문의대응 고객센터
물품의 A/S, 물품의 배송
고지서 및 DM의 발송
법률이 허용한 채권추심업무 등

벌칙조항

▪ 2천만원 이하의 과태료

그 외의 위탁

정보통신망법 제25조 제1항

그 외의 개인정보 취급위탁은 아래
사항을 고지하고 이용자 동의 취득
1 취급위탁을 받는 자 (수탁자)
2 취급위탁 업무 내용

그 외에 서비스 제공에 관한 계약
이행에 필요하지 않은
개인정보 취급위탁 일체

▪ 5년 이하 징역 또는
5천만원 이하 벌금

제3자 제공과 취급위탁의 차이점 ?

제3자 제공

개인정보를 제3자에게 제공

개인정보를 받아간 제3자는
제3자(자신) 업무에 개인정보 활용

예시)
쇼핑센터가 보험사와 업무제휴를
맺고 개인정보를 보험사에 제공한뒤
보험사는 자사 영업에 활용

제3자 취급위탁

개인정보를 제3자에게 제공

개인정보를 받아간 제3자는
위탁자의 업무에 개인정보를 활용

예시)
쇼핑센터가 고객센터와 위탁계약을
맺고 개인정보를 고객센터에 제공한 뒤
고객센터는 쇼핑센터 상담업무에 활용

개인정보 취급 위탁시 유의할 점

주요내용

수탁자의 의무

개인정보 취급위탁을 받은 수탁자에게도
정보통신망법의 개인정보보호 규정이 모두 적용됨

관리감독

준용사업자는 수탁자가 법 규정을 위반하지 않도록 하기 위해
관리 감독할 책임이 있음
(양벌 규정이 적용될 경우, 관리감독을 잘 했는지 여부가 관건)

준용사업자 책임

수탁자가 법 규정을 위반하여 이용자에게 손해를 끼치면
그 수탁자를 준용사업자의 소속 직원으로 봄
(수탁자의 위반행위는 준용사업자 본사의 책임이 됨)

개인정보 취급위탁 위반사례



A 사업자

택배업무를 위탁하고
고객정보 DB를 제공



B 택배업체

개인정보 DB를 넘겨주고
자신들이 배송을 전담하기로 협의



고객정보를
인터넷쇼핑몰에 유출

영업을 양도, 합병하기 위해서는

주요내용

관련조항

정보통신망법 제26조

원칙

영업을 양도, 합병하게 되어 개인정보를 이전하는 경우는
아래 사항을 이용자에게 통지

1. 개인정보 이전 사실
2. 개인정보의 이전을 받는 자 (영업 양수자) 주소, 전화번호
3. 이용자가 개인정보 이전을 원치 않는 경우 **동의철회 방법**

참고사항

원칙적으로는 개인정보 이전을 받은 자(영업 양수자)도 이용자에게 통지
하여야 하나, 양도자가 통지한 경우는 **양수자는 통지 의무 면제**

통지방법

전자우편, 서면, FAX, 전화 기타 이와 유사한 방법

벌칙조항

2천만원 이하의 과태료

7. 영업의 양도, 합병

수집

이용 및
제공

저장 및
관리

파기

영업 양도 통지 위반 사례



인터넷 서비스를 이용 하고 있다가
양도된 사실을 뒤늦게 알게 되었음

Y유선방송은 X통신사업자에게
양도되었으나, 서비스 양도에
대한 사실을 고지하지 않음

Y 유선방송



X 통신사
양도



8. 관리책임자와 취급방침

수집

이용 및
제공

저장
및 관리

파기

개인정보 관리책임자 지정과 개인정보 취급방침 게재

개인정보 관리책임자

개인정보 취급방침

관련조항

정보통신망법 제27조

정보통신망법 제27조의2

원칙

준용사업자는 개인정보관리
책임자를 지정해야 함

준용사업자는
개인정보 취급방침을 정하여
공개해야 함

특이사항

종업원 5인 미만의 준용사업자는
사업주나 대표자가 자동적으로
개인정보 관리책임자가 되며
별도 지정절차는 필요치 않음

- 인터넷 페이지가 없는 사업자는
점포, 사업소에 비치, 열람
- 인터넷 페이지와 점포, 사업소가 모두
있는 사업자는 하나 이상의 방법으로
취급방침을 공개

벌칙조항

2천만원 이하의 과태료

2천만원 이하의 과태료

관리적, 기술적 보호조치 개요

내용	
관련조항	정보통신망법 제28조
원칙	관리적 조치 1. 내부관리계획의 수립 및 시행 2. 개인정보 관리책임자 의무, 책임에 대한 내부 지침 마련 3. 잠금장치 등 물리적 접근방지 조치 4. 개인정보보호를 위한 정기적인 자체 감사 실시 등 기술적 조치 1. 개인정보에 대한 접근 권한을 확인하기 위한 식별 및 인증 조치 2. 권한 없는 접근 차단을 위한 암호화와 방화벽 설치 3. 접속기록의 위조·변조 방지를 위한 조치 4. 침해사고 방지를 위한 보안프로그램의 설치 및 운영 등
특이사항	준용사업자에 대해서는 관리적, 기술적 보호조치가 선별 적용될 수 있음 (홈페이지가 없는 준용사업자 등은 기술적 조치 미적용)
벌칙조항	보호조치 위반으로 개인정보 유출시 5년 이하 징역 또는 5천만원 이하 벌금 보호조치 위반에 대해서는 3천만원 이하 과태료

직원의 개인정보 관리 책임

	내용
관련조항	정보통신망법 제28조의2
원칙	개인정보를 취급하는 직원은 직무상 알게 된 개인정보 를 훼손, 침해, 누설하여서는 안됨
특이사항	• 퇴사하였거나 과거 그 직무를 수행했었던 자도 적용됨 • 직원의 개인정보 누설 사정을 알면서도 개인정보를 제공받은 자도 마찬가지로 처벌 (공모에 의한 유출 방지)
벌칙조항	5년 이하의 징역 또는 5천만원 이하의 벌금 (직원 개인)

수집

이용 및
제공

저장
및 관리

파기

직원의 개인정보 유출 사례



A 아울렛 직원이 퇴사 시
고객 정보를 가져감



B 아울렛으로
이직



이용하지 않던 B 아울렛으로
부터 회원카드 수령

회원카드 발급



개인정보 침해에 대한 양벌 책임

	내용
관련조항	정보통신망법 제75조
원칙	법인의 대표자, 법인이나 개인(사업주)의 대리인, 사용인, 종업원이 개인정보 법 규정을 위반한 경우 행위자 외에 그 법인에게도 벌금형 부과
쟁점사항	법인이나 개인이 종업원에 대해 관리 감독 책임을 다하였음에도 벌금형을 부과하는 것이 타당한지 여부가 사회 쟁점화 ⇒ 법인 또는 개인(사업주)가 위반행위 방지를 위해 상당한 주의감독 을 기울인 경우에는 처벌을 면제 하는 규정 신설
벌칙조항	5년 이하의 징역 또는 5천만원 이하의 벌금 (직원 개인) 5천만원 이하의 벌금 (법인 또는 개인사업주)

수집

이용 및
제공

저장
및 관리

파기

양벌책임 적용사례



택배업체

택배업무 위탁



택배 수탁업체

개인정보
유출

법원은 주의감독 의무 소홀을 이유로
양벌규정을 적용하여 택배업체에 벌금형 부과



인터넷 홈쇼핑

개인정보 파기는 어떻게 ?

	주요내용
관련조항	정보통신망법 제29조
원칙	정보통신서비스제공자는 이용자의 개인정보를 수집,제공받은 목적을 달성한 경우 개인정보를 “ 지체 없이 ” 파기
주요예외	다른 법률 에 따라 개인정보를 보존하여야 하는 경우 - 상법, 전자상거래소비자보호법 등 - 개인정보를 일정기간 보관하도록 규정 (약 3~5년)
파기방법	▪ 문서 : 분쇄 또는 소각 ▪ 전자적 파일형태 : 재생할 수 없는 기술적 방법을 사용하여 파기
벌칙조항	3천 만원 이하의 과태료

개인정보 파기 미흡 사례



생각해 볼 점

- “회원탈퇴”를 하면 무조건 개인정보를 파기해야 한다 ?
 - 회원탈퇴나 거래 종료가 되었더라도
미납요금의 정산, 제품이나 서비스의 A/S 등이 남아있다면
수집, 제공받은 목적이 달성된 것이 아니므로
개인정보 파기를 하지 않는 경우도 있음
- 다른 법률에서 개인정보 보관 사유를 정한 경우도 있음
- 최초에 개인정보 수집시 “수집, 이용목적” 및 “보관기간”을
잘 설정하여 동의를 받으면 파기에 따른 문제를 해결할 수 있음

3 관리적, 기술적 보호조치

내부관리계획의 수립 및 시행

내부 관리계획

- 개인정보 안전성 확보를 위한 **내부 관리계획**을 수립하고 최고 경영층의 승인을 받아 시행
- 사내 개인정보보호 관리책임자(CPO)의 지정
- 개인정보취급자(직원)의 교육에 관한 사항
- 관리적, 기술적 보호조치 내역 및 이행여부 점검
- 자체적인 개인정보보호 감사에 관한 사항



물리적 접근방지 조치

접근방지 조치

- 개인정보 DB에 대한 **인적, 물리적 접근통제** 를 의미함
- 개인정보 DB 시설, 문서 보관장소 등에 대한 통제
- 개인정보취급자에 대한 접근권한 부여 및 제한
- 접근권한 미취득자, 권한 제한자의 출입, 접근 통제
- 재해에 대한 대비 조치



관리적 보호조치 미흡 사례

개인정보 명부 관리, 파기에 대한 **내부관리계획** 부재

문서 보관장소에 대한 **접근통제** 미비



**고객 가입신청서 명부가
폐지상에서 발견**

접근권한 통제

접근권한 관리

- 개인정보처리시스템 접근권한을 제한하여 부여
- 개인정보처리시스템에 대한 **접근권한 차등 관리**
- 책임자/취급자의 전보, 퇴직시 지체없이 변경, 말소

비밀번호 관리

- 개인정보처리시스템에 접근하기 위한 취급자의
비밀번호는 **일정 기준 이상**으로 설정
- 비밀번호 유효기간을 설정하고 반기별 1회 변경 권고

권한없는 외부접근 통제

- 취급중인 개인정보가 홈페이지 등을 통해
외부의 열람권한 없는 자에게 공개, 유출되지 않도록
접근권한 설정

권한없는 접근 차단

침입차단,
탐지시스템
설치

- 개인정보처리시스템에 대한 권한없는 접근 차단을 위해 **침입차단/탐지 시스템** 설치 운영

저장, 전송시
암호화

- 저장 보관중인 개인정보 암호화
- 개인정보 송.수신시 암호화 (보안서버)

1) SSL 인증방식 보안서버 2) 응용프로그램 방식 보안서버



접속기록 위변조 방지, 보안프로그램

접속기록 위변조 방지

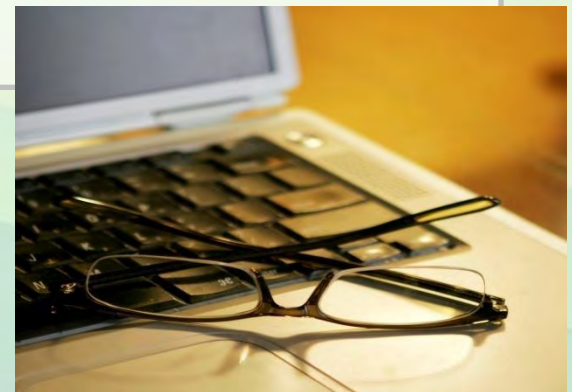
- 개인정보취급자가 개인정보처리시스템에 접속, 처리한 내역을 보관 및 주기적 감독, 확인

최소 6개월 이상 보존, 월 1회 이상 확인, 감독
접속기록 위변조 방지를 위해 별도의 물리적 저장장치에 보관

보안 프로그램 설치운영

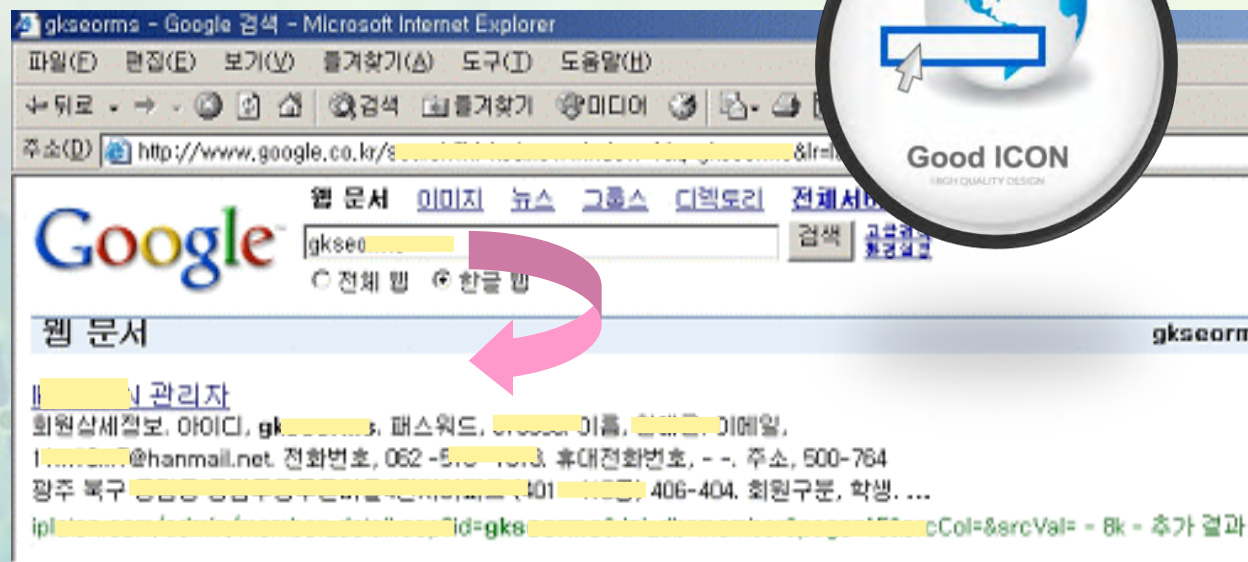
- 바이러스, 악성코드 대응을 위한 백신 S/W 설치운영

월 1회 이상 주기적으로 갱신, 점검
운영체제 및 백신 S/W 제작사의 업데이트 반영, 갱신



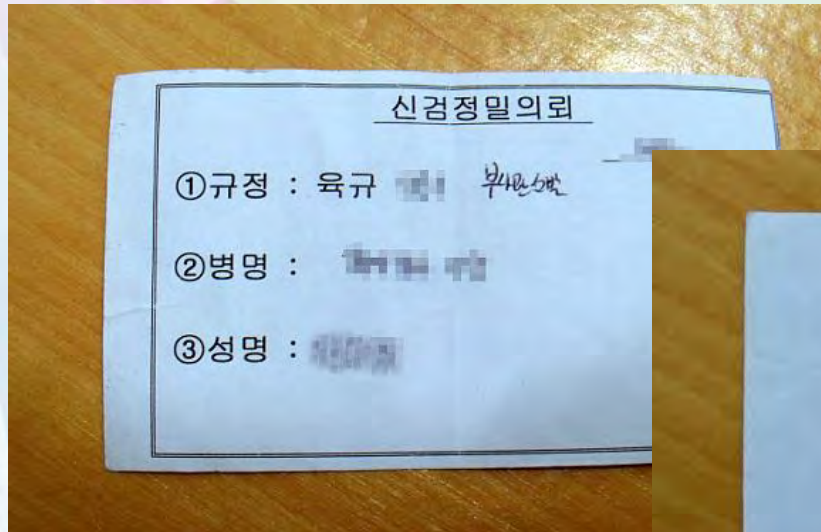
기술적 보호조치 미비 사례

개인정보처리시스템에 대한 외부인의 **접근통제** 미흡으로
인터넷 검색사이트를 통해 개인정보 DB 노출



출력물 보호조치 미흡 사례

개인정보가 인쇄된 **출력물** 관리 미흡



2	2	최	0116-11	22	신경외과
2	2	최	0612-11	25	내과
2	2	이	1018-14	14	정형외과
2	2	고	0614-11	15	내과
2	2	권	0307-11	15	정신과
2	2	김	0630-16	218	정신과
2	2	박	0103-17	10	피부과
2	2	이	1107-11	14	정신과
2	2	조	1012-16	14	정신과
2	2	김	1011-11	48	정신과
2	2	박	1012-17	21	신경외과
2	2	이	0116-19	119	신경외과
2	2	이	070318-16	119	내과
2	2	강	10917-10	17	내과, 정신과
2	2	배	0920-12	27	내과
2	2	김	1031-13	10	내과
2	2	서	0009-16	17	정신과
2	2	박	11227-19	26	정신과, 치과
2	2	권	0527-16	11	내과
2	2	이	0531-11	13	신경외과
2	2	황	01119-11	19	신경외과

출처 : 다음 아고라 제보게시판

4 개인정보보호법

시행으로 바뀌는 점

1) 법 적용대상 확대와 보호체계 변화

적용대상 확대

공공, 민간사업자, 비영리단체를 불문하고, 업무상 필요에 따라 개인정보를 수집, 취급하는 **모든 자**는 개인정보보호법 적용을 받음

보호체계 변화

행정안전부가 국가 개인정보보호 제도 운영을 총괄하고
국무총리 소속 **개인정보보호 위원회** 신설

2) 개인정보 유출통지 제도 신설

개요

개인정보 처리자(사업자, 공공기관 등)은 개인정보 유출사고 발생시 지체없이 정보주체(이용자)에게 **유출 사실을 통지**

통지항목

- 1) 유출 개인정보 항목
- 2) 유출 시점, 유출 경위
- 3) 피해 최소화 등의 방법
- 4) 대응조치 및 피해구제 방법
- 5) 신고접수 연락처

쟁점

- 1) 사업자도 유출 사실을 몰랐을 경우의 통지 책임은 ?
- 2) 유출 사실을 통지하면 책임이 감면될 수 있는가 ?

3) 고유 식별번호 처리 제한

개요

법률에 따라 부여된 **고유 식별번호**는 특별한 예외사유를 제외하고 원칙적으로 수집, 이용, 취급이 금지됨 (주민번호 등)

처리 예외사유

- 1) 정보 주체에게 별도로 동의를 받은 경우
- 2) 법률이 고유식별정보의 수집, 처리를 규정한 경우
- 3) 공공기관이 소관업무 수행을 위해 불가피하게 수집, 취급해야 하는 경우

고맙습니다