PERSONAL INFORMATION PROTECTION EDUCATION

중소·스타트업 사업자를 위한

개인정보보호 교육

개인정보보호위원회

KISA 한국인터넷진흥원

중소·스타트업 사업자 대상
개인정보보호 교육

CONTENTS

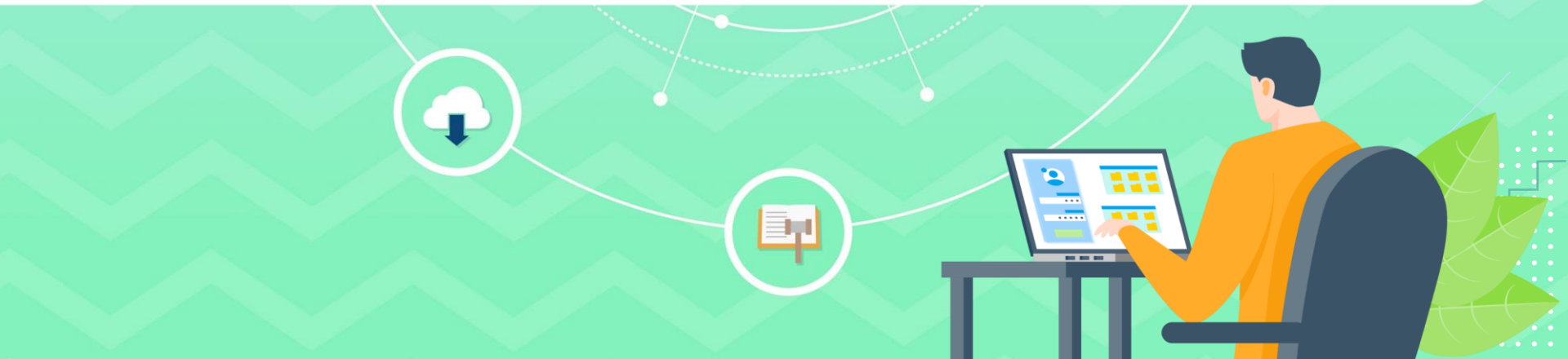
개인정보보호위원회

KISA 한국인터넷진흥원

I

개인정보의 정의와 기본 원칙

중소·스타트업 사업자 대상 개인정보보호 교육



1 개인정보의 개념

개인정보란?

개인정보란?


기 존
개인을
알아볼 수 있는 정보
식별 가능성이 있는 정보
개인을 알아볼 수 없는 정보
(비식별 정보)
개 정
개인정보
영역
개인을 알아볼 수 있는 정보
식별 가능성이 있는 정보
가명정보
일반정보
영역
익명정보

[참고] 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 정보**라 할 것이므로 정보통신망법 제2조 제1항 제6호에서 정한 개인정보에 해당

(서울중앙지법 2007. 2. 8. 선고 2006가합33062, 53332 참조)

[참고] 관련 판례 (1)

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 더더욱 그러할 가능성이 높으며,
설령 휴대전화번호 뒷자리 4자만으로 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…개인정보 보호법 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.

2 개인정보의 유형과 분류

통신·위치 정보

통화·문자내역, IP주소,
화상정보, 위치 정보

일반적 정보

주민등록번호,
이름, 주소, 가족관계 등

사회적 정보

교육 정보,
근로 정보, 자격 정보

정신적 정보

기호, 성향, 신념, 사상

재산적 정보

개인금융정보,
신용정보

신체적 정보

신체정보,
의료·건강정보

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

4 개인정보 자기결정권

개인정보에 대한 인식

과거 ····· 소극적 개념

개인의 사적인 생활을
남에게 방해 받지 않을 권리
(Privacy)

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

II

개인정보 보호법 개정 현황

중소·스타트업 사업자 대상 개인정보보호 교육

1 개인정보 보호법 주요 개정 내용

개인정보 보호 감독기구의 일원화

개인정보 보호 기능의 분산

개인정보보호위원회	행정안전부	방송통신위원회
✓ 심의·의결 기능 정부위원회	✓ 공공·민간(오프라인) 관리감독	✓ 민간(온라인) 관리감독
✓ 헌법기관, 중앙행정기관, 지자체 등에 대한 시정권고	✓ 개인정보 보호법	✓ 정보통신망법

개인정보보호 관련 업무를 보호위원회로 통합·이관

- 개인정보보호위원회를 중앙행정기관으로 격상
- 각 부처의 개인정보보호 업무 통합
- 안전한 데이터 활용을 위한 감독체계 구축

1 개인정보 보호법 주요 개정 내용

정보통신망법과 개인정보 보호법의 통합

개정 이전

- 개인정보 보호법 (일반법)
- 정보통신망법 (특별법)

개정 이후

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
- 유출통지 및 신고
- 개인정보 유효기간제
- 동의철회
- 이용내역통지
- 손해배상 보험
- 노출개인정보 삭제·차단
- 국내대리인
- 국외이전
- 상호주의
- 과징금
- 방송사업자 준용

정보통신망법과 개인정보 보호법의 통합

(이전) 정보통신망 이용촉진 및 정보보호 등에 관한 법률	(개정) 개인정보 보호법
제22조 (개인정보의 수집 · 이용 동의 등)	제39조의3 (개인정보의 수집 · 이용 동의 등에 대한 특례)
제24조의2 (개인정보의 제공 동의 등)	제18조(개인정보의 목적 외 이용 · 제공 제한) 제2항 단서 규정
제27조의3 (개인정보 유출등의 통지 · 신고)	제39조의4 (개인정보 유출 등의 통지 · 신고에 대한 특례)
제28조 (개인정보 보호조치)	제39조의5 (개인정보의 보호조치에 대한 특례)
제29조 (개인정보의 파기)	제39조의6 (개인정보 파기에 대한 특례)
제30조 (이용자의 권리 등)	재39조의7 (이용자의 권리 등에 대한 특례)
제30조의2 (개인정보 이용내역의 통지)	제39조의8 (개인정보 이용내역의 통지)
제32조의3 (손해배상의 보장)	제39조의9 (손해배상의 보장)
제32조의4 (노출된 개인정보의 삭제 · 차단)	제39조의10 (노출된 개인정보의 삭제 · 차단)
제32조의5 (국내대리인의 지정)	제39조의11(국내대리인의 지정)
제63조 (국외 이전 개인정보의 보호)	제39조의12 (국외 이전 개인정보의 보호)
제63조의2 (상호주의)	제39조의13 (상호주의)
제67조 (방송사업자에 대한 준용)	제39조의14 (방송사업자 등에 대한 특례)
제64조의3 (과징금의 부과 등)	제39조의15 (과징금의 부과 등에 대한 특례)

1 개인정보 보호법 주요 개정 내용

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 개인**을 알아 볼 수 없도록 처리하는 것 *(개인정보 보호법 개정 제2조)*

가명정보의 처리

① 통계작성, ② 과학적 연구, ③ 공익적 기록보존 등의 목적으로 정보주체의 동의 없이 가명정보 처리 가능

(개인정보 보호법 개정 제28조의 2(가명정보의 처리 등))

1 개인정보 보호법 주요 개정 내용

데이터의 이용 제공 범위 확대

개인정보의 이용·제공 범위 확대

개인정보의 수집목적 범위 내 이용·제공 가능 (제15조, 제17조)

동의없이

개인정보의 수집목적과 합리적으로 관련된 범위 내 이용·제공 가능 (제15조 제3항, 제17조 제4항)

가명정보의 이용·제공 범위 확대

통계 작성 및 학술 연구 등 (제18조 2항 4호)

통계작성, 과학적 연구, 공익적 기록 보존 등 (제28조의2 1항)

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

1 개인정보 보호법 주요 개정 내용

가명정보의 데이터 결합 시 법적 근거 제시

데이터 결합에 대한 명시적인 법적 근거 부재 → 정보 집합물 결합에 대한 법적 근거 명시

- **기업 내부의 가명정보는 자체적으로 결합**(제28조의2)**하도록 하되, 서로 다른 기업간 가명정보의 결합은 보안시설을 갖춘 전문기관 내에서 수행**(제28조의3 제1항)
  ※ 전문기관은 보호위원회 또는 관계 중앙행정기관의 장이 지정
- **결합을 수행한 기관 외부로 결합된 정보를 반출할 경우 가명 또는 익명 조치 후 전문기관의 승인을 거쳐 반출 가능**(제28조의3 제2항)
- **가명정보의 결합 절차 및 방법**(고시)
- **결합전문기관(반출심사위원회)의 결합정보 반출 승인 기준**(영 제29조의3제4항)

결합 목적과 반출 정보가 관련성이 있을 것	특정 개인을 알아볼 가능성이 없을 것	반출 정보에 대한 안전조치 계획이 있을 것

가명정보의 안전조치 요구사항

- 가명정보에 대한 안전조치 의무를 부과하고 위반시 과태료 및 형사벌 부과
- 재식별을 금지하고 위반시 과징금 및 형사벌 부과

가명정보 안전조치 의무(제28조의4)

- 원 상태로 복원하기 위한 추가정보를 별도로 분리·보관 관리
- 분실·도난·유출·위조·변조·훼손되지 않도록 기술적, 관리적, 물리적 조치
- 가명정보 처리 기록을 작성·보관

위반시

2년 이하 징역 또는 2천만원 이하 벌금 및
3천만원 이하 과태료 부과

가명정보 처리시 금지 의무(제28조의5)

- 특정 개인을 알아보기 위한 목적으로 가명 정보 처리 불가
- 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 처리 중지, 회수·파기

위반시

4억원 이하 또는 전체매출 3% 이하 과징금
5년 이하 징역 또는 5천만원 이하 벌금

가명정보의 안전조치 요구사항

- 추가정보를 별도로 분리·보관 관리
- 가명정보 처리기록의 작성·보관

추가정보를 별도로 분리.보관 관리(영 제 29조의5)

- 가명정보와 추가정보의 분리·보관
- 가명정보와 추가정보에 대한 접근권한의 분리

가명정보 처리 기록의 작성·보관(영 제29조의5)

- 가명정보 처리의 목적
- 가명처리한 개인정보의 항목
- 가명정보의 이용내역
- 제3자 제공 시 제공받는 자
- 보호위원회가 필요하다고 인정하여 고시하는 사항

데이터의 이용 제공 기준

법률에서 위임한 사항에 대한 규정

기존

개인정보 이용·제공 조건

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

개정

(동의없이) 개인정보 이용·제공 기준 추가

- **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 개인정보 보호법 시행령 개정 현황

민감정보의 범위 변경

기 존	개 정
민감정보의 범위	**민감정보의 확대**
▪ 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보	▪ **개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 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	▪ **인종이나 민족에 관한 정보**

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

2 개인정보 보호법 시행령 개정 현황

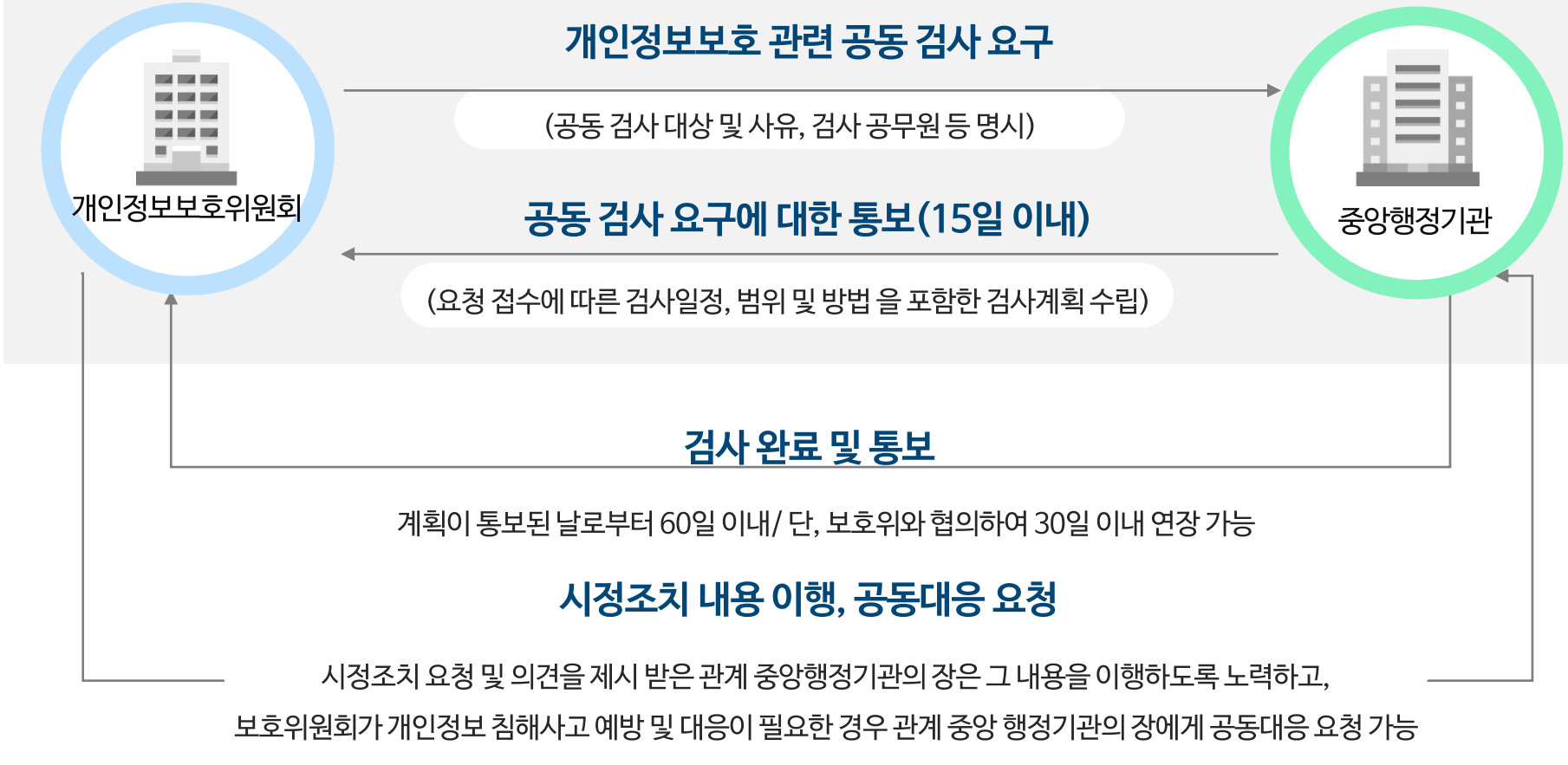
가명정보의 결합 및 안전한 관리 등에 관한 사항 규정

세부 사항

결합정보의 관리와 전문기관 지정	▪ 결합전문기관과 결합키 관리기관의 분리 ▪ 가명정보 및 추가정보에 대한 안전성 확보조치 기준 ▪ 가명정보 결합을 위한 세부 절차와 방법 ▪ 결합된 정보의 반출 승인 기준 ▪ 가명정보 결합전문기관의 지정 및 취소 관련 사항
가명정보의 안전성 확보조치	▪ 가명정보 또는 추가정보에 대한 접근권한 관리 및 물리적 기술적 안전조치에 관한 내부 관리 계획수립 ▪ 가명정보의 처리목적, 처리 및 보유기간, 추가 정보의 이용 및 파기에 관한 사항
결합전문기관에 대한 관리감독 사항	▪ 결합전문기관에 대한 가명정보의 안전한 처리 (ex : 가명정보의 결합 및 반출 승인 과정에서의 법 위반) 에 대한 관리감독 기준 ▪ 가명정보의 안전한 처리를 위한 결합전문기관에 대한 관리감독 기준 ▪ 가명정보 처리에 대한 과징금 부과기준

2 개인정보 보호법 시행령 개정 현황

보호위원회의 공동 검사 요구 방법·절차 규정



III

개인정보 보호법 특례 규정과 개인정보 처리 기준

중소·스타트업 사업자 대상 개인정보보호 교육

특례 규정의 적용 대상 및 범위(정보통신망법 제2조)

적용서비스 : 정보통신서비스

- 「전기통신사업법」 제2조제6호에 따른 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것

의무주체 : 정보통신서비스 & 정보통신서비스 제공자 등

- 「전기통신사업법」 제2조제8호에 따른 전기통신사업자
- 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자
- 정보통신서비스 제공자와 그로부터 이용자의 개인정보를 제공받은 자 (법 제39조의4)

보호주체 : 정보통신서비스 이용자

- 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자

2 개인정보 수집 이용(제39조의3)

이용자의 개인정보를 수집하는 경우 일정 사항을 이용자에게 알리고 동의를 얻어야 함

(원칙) 이용자의 동의

- 동의를 받을 때 고지사항
  (위반 시 3천 만원 이하의 과태료)

① 개인정보의 수집·이용 목적

② 수집하는 개인정보의 항목

③ 개인정보의 보유 및 이용 기간

[예외] 이용자 동의 없이 수집할 수 있는 경우

- 정보통신서비스의 제공에 관한 **계약을 이행하기** 위하여 필요한 경우 (단, 경제적 · 기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우)
- 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
- 다른 법률에 특별한 규정이 있는 경우

위반 시 5년 이하의 징역 또는 5천만원 이하의 벌금

3 개인정보 수집 제한(제39조의3)

**필요한 최소한의 개인정보만을 수집하고,
필요한 최소한의 개인정보 이외의 개인정보를 제공하지 않는다는
이유로 그 서비스의 제공을 거부해서는 안 됨**

필요한 최소한의 개인정보만 수집

- 필요한 최소한의 개인정보
- 해당 서비스의 본질적 기능 수행을 위해 반드시 필요한 정보

필요한 최소한의 개인정보 외의 개인정보 제공 거부 가능

- 개인정보를 제공하지 아니한다는 이유로 그 서비스 제공 거부 불가

서비스 제공을 거부한 자는 3천만원 이하의 과태료 부과

[참고] 온라인 개인정보 처리 가이드라인

1. 필수·선택동의 항목을 엄격하게 구분 : 필수항목은 해당 서비스의 본질적인 기능

(예시 1) 온라인 쇼핑몰의 경우 결제·배송정보는 인터넷 회원가입 단계에서는 필수동의 항목으로 볼 수 없으나, 선택동의 항목으로 분류하여 이용자의 동의를 받은 경우에는 인터넷 회원가입 단계에서 수집·이용 가능

(예시 2) 서비스 제공 과정에서 명의도용·개인정보 유출 등 방지를 위한 '본인확인' 기능은 서비스의 특성에 따라 본질적 기능으로 분류할 수 있음 -〉 회원가입단계에서 불필요한 본인확인은 바람직하지 않으나 법령상 의무이행(연령, 본인확인)은 가능함

(예시 3) 온라인 쇼핑몰에서 비회원 구매의 경우에는 '인터넷 회원가입'이 필요 없으므로 결재·배송 정보만을 수집

(예시 4) 법률에 따라 동의없이 수집한 개인정보는 별도 DB 또는 테이블에 분리하여 저장해야 하고 마케팅 등 다른 목적으로 이용할 수 없음

[참고] 온라인 개인정보 처리 가이드라인

2. 선택동의 항목은 목적 별로 개별 동의하고 마케팅 목적은 분리하여 개별 동의

3. 개인정보가 필요한 시점에 수집

(예시 1) 회원제 서비스를 제공하는 온라인 쇼핑몰의 경우 가입시점에는 아이디, 비밀번호 등 회원 가입에 필요한 최소 정보만 수집하며 물건 구매 시 비로소 배송, 결제정보 수집.
다만 가입 시점에서 선택동의 사항으로 배송, 결제정보를 받는 것은 가능

4. 과도한 개인정보 수집 지양 : 비회원과 회원의 정보를 동일하게 받으면 과도한 개인정보 수집

5. 서비스 본질과 무관한 정보는 마스킹 처리

[참고] 온라인 개인정보 처리 가이드라인

6. 영업점의 개인정보 수집·보관 최소화 : 내부관리계획에 반영

(예시 1) 영업점에서 이용자가 개인정보를 전자기기에 입력하면, 본사에 직접 전송되고 영업점에서는 저장되지 않도록 조치

(예시 2) 영업점에 대한 주기적인 개인정보 관리 실태점검 실시

(예시 3) 본사가 텔레마케팅에 대한 동의를 받은 경우라도, 본사가 지정한 영업점에 한하여 텔레마케팅을 할 수 있도록 엄격히 제한하여 영업점의 개인정보 이용 범위를 제한

7. 개인정보 분리 보관시 업무담당자만 열람 가능 해야 하며 영업부서의 접근 제한

8. 사업자(A)가 이용자의 개인정보를 제3자(B)에게 제공한 경우,
이용자는 사업자(A)와 제3자(B) 에게 선택적으로 개인정보 파기 요청 가능

[참고] 온라인 개인정보 처리 가이드라인

9. 개인정보 업무 위탁 시, 위탁자는 수탁자의 개인정보 파기여부 확인

10. 모바일기기에서 개인정보 동의 시 최소한의 사항 고지 후 별도 웹사이트에서 안내하는 것이 바람직 함

11. 이용자의 선택권이 보장된 경우에는 이용자 편의 제공을 위해 여러 동의사항에 대하여 일괄동의 기능을 도입하여 운영할 수 있음

4 14세 미만 아동의 보호(제39조의3)

14세 미만 아동의 개인정보 수집·이용·제공 시 법정대리인(부모 등)의 동의를 얻어야 함

법정대리인의 동의 획득 방법 (예시)

- **법정대리인** : 친권자(부모) 및 후견인

① **지정후견인** → ② **법정후견인** : 직계혈족, 3촌 이내의 방계혈족 순 → ③ **선정후견인**

- 국가 또는 지방자치단체가 설치·운영하는 보호시설에 있는 고아 : **보호시설의 장**

아동에 대한 개인정보 처리와 관련한 사항의 고지 방법

- 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어 사용
- 개인정보 수집 매체의 특성상 동의 내용을 전부 표시하기 어려운 경우 법정대리인에게 동의 내용을 확인할 수 있는 방법(인터넷주소 · 사업장 전화번호 등)을 안내 가능

법정대리인의 동의를 받지 않거나 동의를 확인하지 아니한 경우

5년 이하 징역, 5천만원 이하 벌금

법정대리인의 동의 획득 방법 (예시)

1. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 정보통신서비스 제공자 등이 그 동의 표시를 확인했음을 법정대리인의 휴대전화 문자메시지로 알리는 방법
2. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 신용카드·직불카드 등의 카드정보를 제공받는 방법
3. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 휴대전화 본인인증 등을 통해 본인 여부를 확인하는 방법
4. 동의 내용이 적힌 서면을 법정대리인에게 직접 발급하거나, 우편 또는 팩스를 통하여 전달하고 법정대리인이 동의 내용에 대하여 서명날인 후 제출하도록 하는 방법
5. 동의 내용이 적힌 전자우편을 발송하여 법정대리인으로부터 동의의 의사표시가 적힌 전자우편을 전송 받는 방법
6. 전화를 통하여 동의 내용을 법정대리인에게 알리고 동의를 얻거나 인터넷주소 등 동의 내용을 확인할 수 있는 방법을 안내하고 재차 전화 통화를 통하여 동의를 얻는 방법
7. 그 밖 제1호부터 제6호까지의 규정에 따른 방법에 준하는 방법으로 법정대리인에게 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

5 개인정보 유출 등의 통지 신고(제39조의4)

개인정보 유출 등의 통지

» 유출 등을 안 때부터 24시간 내 지체없이 이용자에게 통지

통지사항

① 유출 등이 된 개인정보 항목
② 유출 등이 발생한 시점
③ 이용자가 취할 수 있는 조치
④ 정보통신서비스 제공자 등의 대응 조치
⑤ 상담 등을 접수할 수 있는 부서 및 연락처

통지면제

- 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우
- 통지 대신 자신의 인터넷 홈페이지에 30일 이상 게시
- 정당한 사유를 지체없이 보호위원회에 서면으로 소명

개인정보 유출 등의 신고

» 유출 등을 안 때부터 24시간 내 보호위원회 또는 KISA 신고

신고사항

- 통지사항과 동일

통지·신고의 지연 및 보완

» 24시간 내 통지·신고할 수 없는 정당한 사유가 있으면 지체없이 그 사유를 보호위원회에 서면으로 소명

- 유출 등이 된 개인정보 항목 또는 유출 등이 발생한 시점에 관한 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 나머지 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고

위반시 3천 만원 이하의 과태료

통지/신고 의무 위반, 24시간을 경과하여 통지/신고, 정당한 사유를 소명하지 아니하거나 거짓으로 소명

6 개인정보의 안전성 확보 조치(영 제48조의2)

내부관리계획의 수립 · 시행	• 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성 · 운영에 관한 사항 • 개인정보취급자의 교육에 관한 사항 • 보호조치를 이행하기 위하여 필요한 세부 사항
개인정보처리시스템에 대한 불법적인 접근 차단 조치	• 접근 권한의 부여 · 변경 · 말소 등에 관한 기준의 수립 · 시행 • 침입차단시스템 및 침입탐지시스템의 설치 · 운영 • 외부 인터넷망의 차단 : 저장 · 관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 매출액 100억원 이상인 자 • 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정 및 운영 등
접속기록의 위조 · 변조 방지 조치	• 개인정보취급자의 접속일시, 처리내역 등의 저장 및 이의 확인 · 감독 • 별도의 저장장치에 접속기록 백업 보관
개인정보의 안전한 저장 · 전송을 위한 보안조치	• 비밀번호의 일방향 암호화 저장 • 주민등록번호, 계좌정보 및 보호위원회가 정하여 고시한 정보의 암호화 저장 • 개인정보.인증정보의 송 · 수신시 보안서버 구축 등
백신소프트웨어 설치 및 주기적 갱신 · 점검 조치	
그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치	

7 개인정보 유효기간제(제39조의6)

서비스를 1년 동안 이용하지 아니하는 이용자의 개인정보는 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리

장기 서비스 미이용자의 개인정보 파기 또는 별도 보관

- 정보통신서비스를 1년 기간 동안 이용하지 아니하는 이용자의 개인정보
- 1년 경과 후 즉시 파기 또는 다른 이용자 정보와 별도 분리 보관
- 보관기간에 대해 다른 법령 또는 이용자의 요청에 따라 달리 정한 경우는 제외

» 다른 이용자의 개인정보와 분리하여 별도로 저장·관리

파기 또는 별도 보관의 통지 : 기간 만료 30일 전까지 이용자에 통지

- 파기시 : 파기 사실, 기간 만료일, 파기되는 개인정보 항목
- 분리 보관시 : 분리 보관 사실, 기간 만료일, 분리 보관되는 개인정보 항목

파기 등 필요한 조치를 하지 아니한 자는 3천 만원 이하의 과태료

8 이용자의 동의 철회 권리(제39조의7)

이용자는 정보통신서비스 제공자 등에 대하여 언제든지 개인정보 수집·이용·제공 동의를 철회할 수 있음

동의 철회의 요건·시기

- 이용자는 언제든지 개인정보 수집 · 이용 · 제공 등의 동의 철회 가능

동의 철회의 방법

- 동의 철회를 요구하는 방법은 개인정보 수집 방법보다 쉽게 할 것

동의 철회의 요건·시기

- 이용자는 언제든지 개인정보 수집 · 이용 · 제공 등의 동의 철회 가능

<예시>

개인정보 항목	<아이 정보 등록> 아이의 애칭, 성별, 생년월일(생일)
동의일	2020.03.20
동의 철회	동의 철회하기

동의 철회 방법을 제공하지 아니한 자는 3천 만원 이하의 과태료

9 개인정보 이용·제공 내역 통지(제39조의8)

수집한 이용자의 개인정보의 이용내역을 주기적으로 이용자에게 통지해야 함 (연락처 등 이용자에게 통지할 수 있는 개인정보를 수집하지 아니한 경우는 예외)

통지의무 대상 정보통신서비스 제공자 등

전년도 말 기준 직전 3개월간 개인정보가 저장·관리되고 있는 이용자 수가 일일 평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 사업자

통지 항목

① 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목

② 개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 항목

※「통신비밀보호법」 및「전기통신사업법」에 따라 수사기관등에 제공한 정보 제외

통지 방법

전자우편· 서면 등의 방법으로 연 1회 이상 통지

이용내역 미통지시 3천 만원 이하의 과태료

10 손해배상의 보장(제39조의9)

손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 함

손해배상책임 보험, 공제 등의 가입 의무

- 개인정보침해 관련 손해배상, 징벌손해배상(3배 배상), 법정손해배상 보장
- 보험 또는 공제 가입, 준비금 적립
- 보험 또는 공제 가입과 준비금 적립 병행 가능

가입 대상자의 범위 및 기준

- 직전 사업연도의 매출액이 5천만원 이상일 것
- 저장 · 관리되고 있는 이용자 수가 일일평균 1천명 이상일 것(전년도 말 기준 직전 3개월간)

보험, 공제 등의 가입 간주

- 다른 법률에 따라 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립한 경우

보험, 공제 등의 가입 기준

- 보험 또는 공제 가입, 준비금 적립의 최저가입금액은 별도 규정

보험 등 미가입시 2천 만원 이하의 과태료

11 노출 개인정보의 삭제·차단(제39조의10)

**이용자의 개인정보가 노출되지 아니해야 하고,
삭제·차단 등 필요한 조치를 취해야 함**

개인정보 노출방지 의무

의무주체	정보통신서비스 제공자 등
노출방지	주민등록번호, 계좌정보, 신용카드정보 등 이용자의 개인정보
의무사항	정보통신망을 통하여 공중에 노출되지 않도록

노출 개인정보에 대한 조치 의무

삭제 등의 요청	**개인정보보호위원회 또는 한국인터넷진흥원**
조치 내용	삭제·차단 등 필요한 조치

12 국내대리인의 지정(제39조의11)

국내에 주소 또는 영업소가 없는 정보통신서비스 제공자(국외 사업자)에게 국내대리인 지정을 의무화함

해외사업자의 국내대리인 지정 의무

국내에 주소 또는 영업소가 없는 정보통신서비스 제공자 등

한국에 정보통신서비스를 제공하면서 이용자의 개인정보를 처리하여야 하고,

국내에 주소 또는 영업소가 없는 자에 해당하며, 또한 다음 중 어느 하나의 기준에 해당하는 자여야 한다.

① 전년도(법인인 경우에는 전 사업연도) 매출액이 1조원 이상인 자

② 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도) 매출액이 100억 원 이상인 자

③ 전년도말 기준 직전 3개월간의 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만 명 이상인 자

④ 개인정보 보호법을 위반하여 개인정보 침해 사건 · 사고가 발생하였거나 발생할 가능성이 있는 경우로서 관계 물품 · 서류 등 자료의 제출을 요구받은 자

※ 매출액은 전년도 평균환율을 적용하여 원화로 환산

12 국내대리인의 지정(제39조의11)

국내에 주소 또는 영업소가 없는 정보통신서비스 제공자(국외 사업자)에게 국내대리인 지정을 의무화함

국내대리인의 업무

- 개인정보 보호책임자의 업무
- 개인정보유출 통지 · 신고
- 보호위원회가 요구한 관계 물품 · 서류 등의 제출

국내대리인의 자격

- 국내에 주소 또는 영업소가 있는 자

개인정보처리방침 공개

- 국내대리인의 성명
- 국내대리인의 주소, 전화번호 및 전자우편 주소

국내대리인의 행위에 대한 정보통신서비스 제공자 등의 책임

- 국내대리인의 위반 행위는 정보통신서비스 제공자 등의 행위로 간주

국내대리인 미지정시 2천만 원 이하의 과태료

13 국외 이전 개인정보의 보호(제39조의12)

국제계약의 체결 제한

- 개인정보 보호법을 위반하는 사항을 내용으로 하는 국제계약 체결 금지

국외 이전에 대한 동의 면제

- 국외 개인정보 처리위탁·보관 사실을 개별 고지하거나 개인정보처리방침에 공개한 경우

국외 재이전 제한

- 국외 이전을 받은 해당 개인정보를 제3국으로 이전 시 동일 요건 적용

개인정보 국외 이전에 대한 동의

- 국외 제공(조회 포함)·처리위탁·보관시
- 국외 이전 동의시 고지시항

① 이전되는 개인정보 항목
② 이전되는 국가, 이전일시 및 이전방법
③ 이전받는 자의 성명(정보관리 책임자 연락처 포함)
④ 이전받는 자의 이용목적 및 보유·이용 기간

※ 이전받는자와 미리 협의하고 이를 계약내용 등에 반영

국외 이전 시 보호조치 의무

- 개인정보 보호를 위한 안전성 확보 조치
- 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 사항
- 그 밖에 이용자의 개인정보 보호를 위하여 필요한 조치

국외이전에 대한 상호주의(제39조의13)

- 국외 이전을 제한하는 국가의 정보통신서비스 제공자 등에 대하여는 해당 국가의 수준에 상응하는 제한 가능

보호조치를 하지 않고 국외이전시 3천 만원 이하의 과태료
공개하거나 알리지 않고 국외 처리위탁·보관시 2천만원 이하 과태료

14 과징금의 부과(제39조의12)

보호위원회는 다음 중 해당하는 행위가 있는 경우 해당 정보통신서비스 제공자등에게 위반행위와 관련해 과징금 부과

위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액

매출액이 없거나 매출액의 산정이 곤란한 경우에는 4억원 이하의 과징금 부과

- 이 법을 위반하여 개인정보를 목적 외로 이용·제공한 경우
- 법정대리인의 동의를 받지 아니하고 아동의 개인정보를 수집한 경우
- 이용자의 동의를 받지 아니하고 민감정보를 수집한 경우
- 관리·감독 또는 교육을 소홀히 하여 특례 수탁자가 이 법의 규정을 위반한 경우
- 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우로서 안전성 확보조치를 하지 아니한 경우
- 이용자의 동의를 받지 아니하고 개인정보를 수집 또는 국외에 제공한 경우

과징금 부과시 고려 사항

- 위반행위의 내용 및 정도
- 위반행위의 기간 및 횟수
- 위반행위로 인하여 취득한 이익의 규모

15 스마트폰 앱 접근권한 동의(정보통신망법 제22조의2)

이용자의 스마트폰에 서비스 제공을 위하여 앱 설치 시 접근권한이 필요한 경우 필수적/선택적 접근권한을 분류 후 아래 사항을 이용자에게 알리고 동의를 받아야 함

접근권한 획득 시 안내하여야 할 사항

- 가. 접근권한이 필요한 정보 및 기능의 항목
- 나. 접근권한이 필요한 이유
- 다. 접근권한 허용에 대하여 동의하지 아니할 수 있다는 사실
  (해당 접근권한이 서비스 제공에 반드시 필요한 접근권한일 경우 생략)
- 이용자가 반드시 필요하지 않은 접근권한을 설정하는데 동의하지 않는다는 이유로 해당 서비스 제공을 거부하여서는 아니된다

앱 실행 시 접근권한 고지에 대한 예시

〈접근권한 고지내용으로 볼 수 없는 사례〉

〈접근권한 고지내용으로 볼 수 있는 사례〉

1단계 (고지)	2단계 (동의)
[필수적 접근권한] ▪ 저장 권한 : 음반 이미지, 곡 재생파일 임시저장을 위해 접근이 필요합니다. OOO 사용을 위해 다음 권한을 허용해 주시기 바랍니다. 다음	OOO의 다음 작업을 허용하시겠습니까? 저장 권한 사용 거부 허용

출처. 스마트폰 앱 접근권한 개인정보보호 안내서(17.3)

[예시] 스마트폰 앱 접근권한 개인정보보호 안내서

1. 동의 대상 접근권한의 범위는 '앱 서비스 제공자가 앱을 통해 접근할 수 있는' 스마트폰 내에 저장되어 있는 정보와 설치된 기능으로 함
2. 접근권한의 범위

   (이용자 저장 정보) 연락처, 일정, 동영상, 사진, 바이오정보 등

   (자동 저장 정보) 위치정보, 통신기록, 인증정보, 신체활동기록 등

   (단말장치 식별 고유정보) 휴대폰 고유 식별번호(IMEI), MAC 주소 등

   (입력·출력 기능) 영상촬영 기능, 음성인식 기능, 바이오정보 및 건강정보 감지센서 기능 등
3. 스마트워치는 화면 크기 제약 등으로 인해 접근권한에 대한 고지·동의 기능을 당장 구현하기 어려운 점을 고려하여, 우선 필수적 접근권한만 설정하도록 권장
4. 접근권한에 대한 동의는 해당 정보에 대한 수집 동의는 아니므로, 만약 해당 정보가 개인정보 관련 법령에 따라 보호받는 개인정보이고 이를 앱 서비스 제공자가 수집하는 경우에는 앱 또는 홈페이지 등에서 회원가입 시 관련 법령에 따라 개인정보의 수집·이용에 대한 동의를 별도로 받아야 함
5. 선택적 접근권한에 대하여 개별 동의가 불가능한 구글 안드로이드 6.0 미만 버전의 운영체제에서는 앱의 접근권한 설정 시 필수적 접근권한만 설정해야 함

IV

개인정보의 기술적·관리적 보호조치

중소·스타트업 사업자 대상 개인정보보호 교육

1 내부관리계획의 수립·시행 (1)

내부관리계획 포함 내용

내부관리계획서 (예시)

제1조 (목적)
제2조 (개인정보 보호 조직 구성 및 운영)
제3조 (개인정보 보호 교육)
제4조 (개인정보처리시스템 접근통제)
제5조 (접속기록의 위·변조 방지)
제6조 (개인정보의 암호화)
제7조 (악성프로그램 방지)
제8조 (물리적 접근 방지)
제9조 (출력·복사 시 보호조치)
제10조 (개인정보 표시제한 보호조치)
제11조 (개인정보 처리위탁 사업자 관리 등)
제12조 (개인정보 유출 시 대응 매뉴얼)
제13조 (기타 개인정보 보호를 위해 필요한 사항)

필요한 최소한의 개인정보 외의 개인정보 제공 거부 가능

- 개인정보 보호책임자 자격요건 및 지정 관련사항
- 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
- 내부관리계획의 수립 및 승인에 관한 사항
- 개인정보의 기술적·관리적 보호조치 이행여부의 내부 점검에 관한 사항
- 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
- 개인정보의 분실 도난 유출 변조 훼손 등이 발생한 경우의 대응절차 및 방법에 관한 사항
- 기타 개인정보 보호를 위해 필요한 사항

1 내부관리계획의 수립·시행 (2)

개인정보 보호책임자 지정에 관한 사항

개인정보 보호책임자의 자격요건 및 지정에 관한 사항(개인정보보호 제31조(개인정보 보호책임자의 지정)

대표자(사업주) 또는 임원(임원이 없는 경우 개인정보와 관련하여 개인정보 처리 관련 업무를 담당하는 부서의 장)으로 지정

개인정보 보호책임자의 역할 및 책임

- 개인정보 보호 계획의 수립 및 시행
- 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
- 개인정보 처리와 관련한 불만의 처리 및 피해 구제
- 개인정보 유출 및 오용 · 남용 방지를 위한 내부통제시스템의 구축
- 개인정보 보호 교육 계획의 수립 및 시행
- 개인정보파일의 보호 및 관리 · 감독
- 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

개인정보취급자의 역할 및 책임

- 법 제30조에 따른 개인정보 처리방침의 수립 · 변경 및 시행
- 개인정보 보호 관련 자료의 관리
- 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

개인정보의 기술적·관리적 보호조치 이행 여부의 내부 점검에 관한 사항

점검시기	정기적 (최소 연1회 권고)
점검방법	점검시기, 대상, 내용 등을 포함
점검자	사업장 내에 개인정보 보호 관련 부서의 감사자 또는 유관 부서의 전문가로 구성 가능
점검절차	범위, 대상, 기간, 점검수행자 등의 내용과 점검 결과를 어떻게 처리할 것인지의 내용 포함
점검결과 자료관리	시스템 점검 결과 요약, 시스템 로그 및 수집한 증거자료 등 점검 시 생성된 모든 자료와 결과보고서를 관리하는 것을 의미 → 점검결과에 대한 접근은 점검반으로 제한하여 자료의 무결성 보장

개인정보보호 교육 계획 수립 및 기타 개인정보보호 필요 사항

개인정보보호 교육 계획을 수립하고
'사업규모, 개인정보 보유 수 등을 고려하여 특성에 맞는 교육을 정기적으로 실시'

교육 대상 : 개인정보보호책임자, 개인정보취급자

교육계획서에 포함되어야 하는 사항 : 교육대상, 교육목적, 교육내용, 교육일정 및 방법 등

교육은 온라인 등으로도 가능하며 외부기관이나 전문요원에 위탁하여 진행할 수도 있음

기타 개인정보보호를 위해 필요한 사항

보안서약서 작성

임직원 개인정보 보호 인식 제고

중고PC 하드디스크 폐기 방법 등

개인정보처리시스템에 대한 개인정보취급자의 접근권한 관리

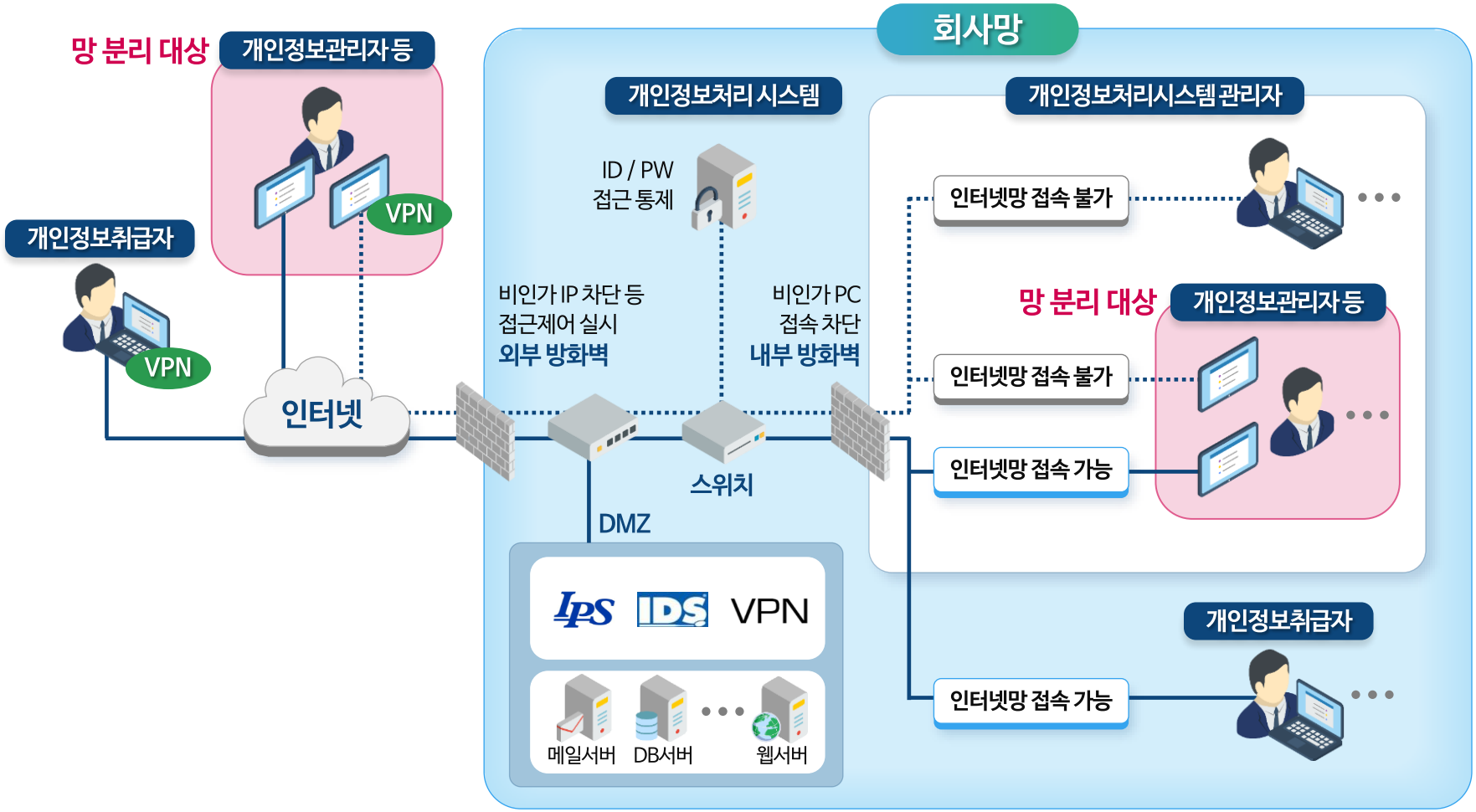
- 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보 보호책임자 또는 개인정보취급자에게만 부여)
- 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소
- 개인정보처리시스템 접근권한의 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관
- 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용
- 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 시스템을 설치·운영
  - 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가 받지 않은 접근 제한
  - 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도 탐지

2 접근통제 (2)

개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단

적용사업자	전년도 말 기준 직전 3개월간 저장·관리되고 있는 개인정보가 일일 평균 100만 명 이상이거나 정보통신서비스 부문 전년도 (법인의 경우에는 전 사업연도) 매출액이 100억 원 이상인 정보통신서비스 제공자 등
적용대상	개인정보처리 시스템에 접근하여 다운로드, 파기 또는 접근권한 설정이 가능한 개인정보취급자의 컴퓨터 등
망 분리 방법	물리적 망 분리 뿐만 아니라 논리적 망 분리도 허용 ※ 일정 수준의 보안성을 갖추었다면 논리적 망 분리도 허용

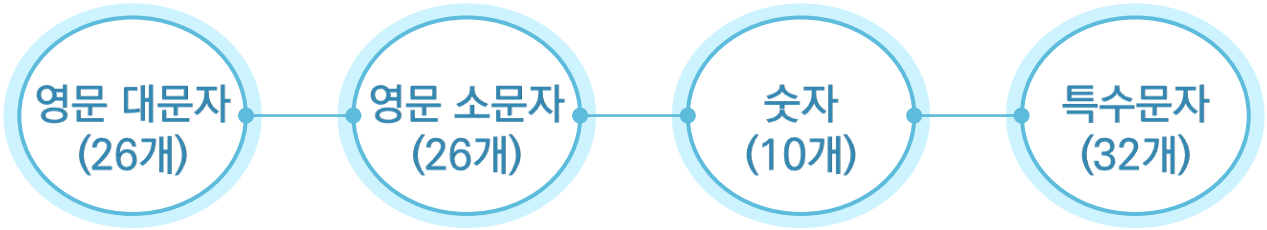
개인정보처리시스템 망 분리 (예시)



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

개인정보처리시스템 및 업무용 컴퓨터 + 모바일 기기 에 대한 개인정보 유출방지 (1)

과실로 인한 인터넷 홈페이지에서 노출 방지

- 웹사이트를 통해 고객의 개인정보를 수집. 관리하는 경우에는 ID 및 비밀번호를 통한 사용자 인증(login) 기능을 적용
- 수시로 웹사이트 게시판 등에서의 주민번호 노출 여부 등을 점검하여 조치

인터넷 홈페이지 취약점으로 인한 노출 방지

- 수시로 인터넷 홈페이지 취약점을 점검하여 조치
- 홈페이지를 개발할 때 KISA가 권고하는 웹 보안 서비스를 따르도록 하여 취약점을 최소화

※ 웹 보안 서비스 : KISA 인터넷침해대응센터 홈페이지 참조(www.krcert.or.kr)

개인정보처리시스템 및 업무용 컴퓨터 + 모바일 기기 에 대한 개인정보 유출방지 (2)

P2P 프로그램에서의 노출

- 개인정보취급자의 컴퓨터는 P2P 프로그램을 사용하지 않는 것이 바람직하나, 반드시 사용해야 할 경우 공유 폴더에 개인정보 파일이 포함되지 않도록 정기적으로 점검
- P2P, 웹하드 등 사용을 제한하는 경우에도 단순히 사용금지 조치를 취하는 것이 아니라 시스템 상에서 해당 포트를 차단하는 등 원천적인 조치를 취하는 것이 필요

공유설정을 통한 노출

- 공유폴더를 사용할 경우 드라이브 전체 또는 불필요한 폴더가 공유되지 않도록 조치하고, 공유폴더에 개인정보 파일이 포함되지 않도록 정기적으로 점검

※ 윈도우: [시작] → [제어판] → [성능 및 유지관리] → [관리도구] → [컴퓨터 관리] 실행 공유 폴더 메뉴에서 확인 가능

개인정보처리시스템 접속기록 관리

개인정보취급자가 개인정보처리시스템에 접속한 기록을 월1회 이상 정기적으로 확인·감독

- 시스템 이상 유무 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리
- 전기통신사업법 제5조의 규정에 따른 기간통신사업자의 경우에는 최소 2년

〈접속기록 항목(예시)〉

정보주체 식별번호	취급자 식별번호	접속일시	접속지	수행업무
123456789	홍길동(HGD)	2013.04.30. 15:00	172.168.168.11	조회(고객응대)

개인정보취급자의 접속기록이 위·변조되지 않도록 별도의 물리적인 저장 장치에 보관 하여야 하며 정기적인 백업 수행

개인정보 저장·전송 시 암호화

개인정보 저장 시 암호화

- 비밀번호
  : 복호화할 수 없도록 일방향 암호화하여 저장
- ① 주민등록번호, ② 신용카드번호, ③ 계좌번호, ④ [바이오정보] ⑤ [여권번호], ⑥ [운전면허번호], ⑦ [외국인등록번호]
  : 안전한 암호알고리즘으로 암호화하여 저장
- 이용자의 개인정보를 컴퓨터, [모바일기기 및 보조저장매체 등]에 저장할 때 이를 암호화

개인정보 전송 시 암호화

- 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화
- ① 웹서버에 SSL(Secure Socket Layer) 인증서 설치
- ② 웹서버에 암호화 응용프로그램 설치

악성프로그램 감염 예방

- 백신 소프트웨어 등의 보안 프로그램을 설치 운영하고, 자동 업데이트 기능을 사용하거나 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지

- 악성 프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 업데이트 실시

7 물리적 접근 방지

개인정보를 보관하고 있는 물리적 보관 장소에 대한 조치

- 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소에 대한 출입통제 절차를 수립·운영
- 개인정보가 포함된 서류, 보조저장매체 등을 잠금 장치가 있는 안전한 장소에 보관
- 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책 마련

유출 사례

- 카드사의 개인정보처리시스템 관리 수탁자 직원에 의한 유출(2014년 1월)
- 통신사 영업점에 방치된 가입신청서 서류 유출 등
- 호스팅사 등에 개인정보 처리를 위탁통신사 영업점에 방치된 가입신청서 서류 유출 한 경우 계약 시 물리적 접근방지 사항 확인

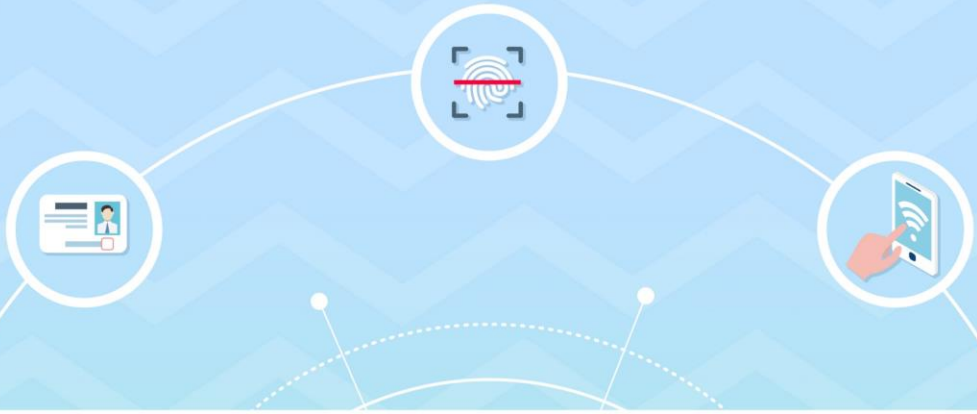
9 출력·복사시 보호조치, 개인정보 표시 제한

개인정보 출력물 보호조치

- 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화
- 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치

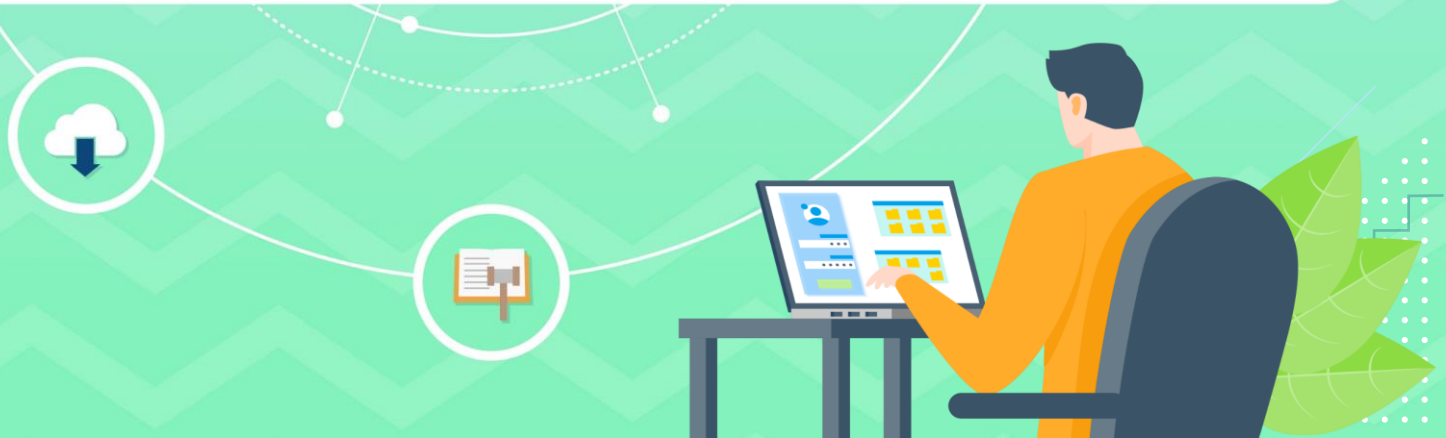
개인정보 표시 제한

- 개인정보 업무처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보보호를 위하여 개인정보를 마스킹하여 표시제한 조치를 취할 수 있다.



질의응답 Q&A

중소·영세 사업자 대상 개인정보보호 교육



Privacy by Trust,
Trust by Privacy.
감사합니다.