



2019년 개인정보 보호법 주요 내용

믿을 수 있는 개인정보 활용, 신뢰사회의 기본입니다

Privacy by Trust, Trust by Privacy

Contents

I . 개인정보 보호의 중요성

II . 총칙

III . 개인정보 보호 정책의 수립 등

IV . 개인정보의 처리

V . 개인정보의 안전한 관리

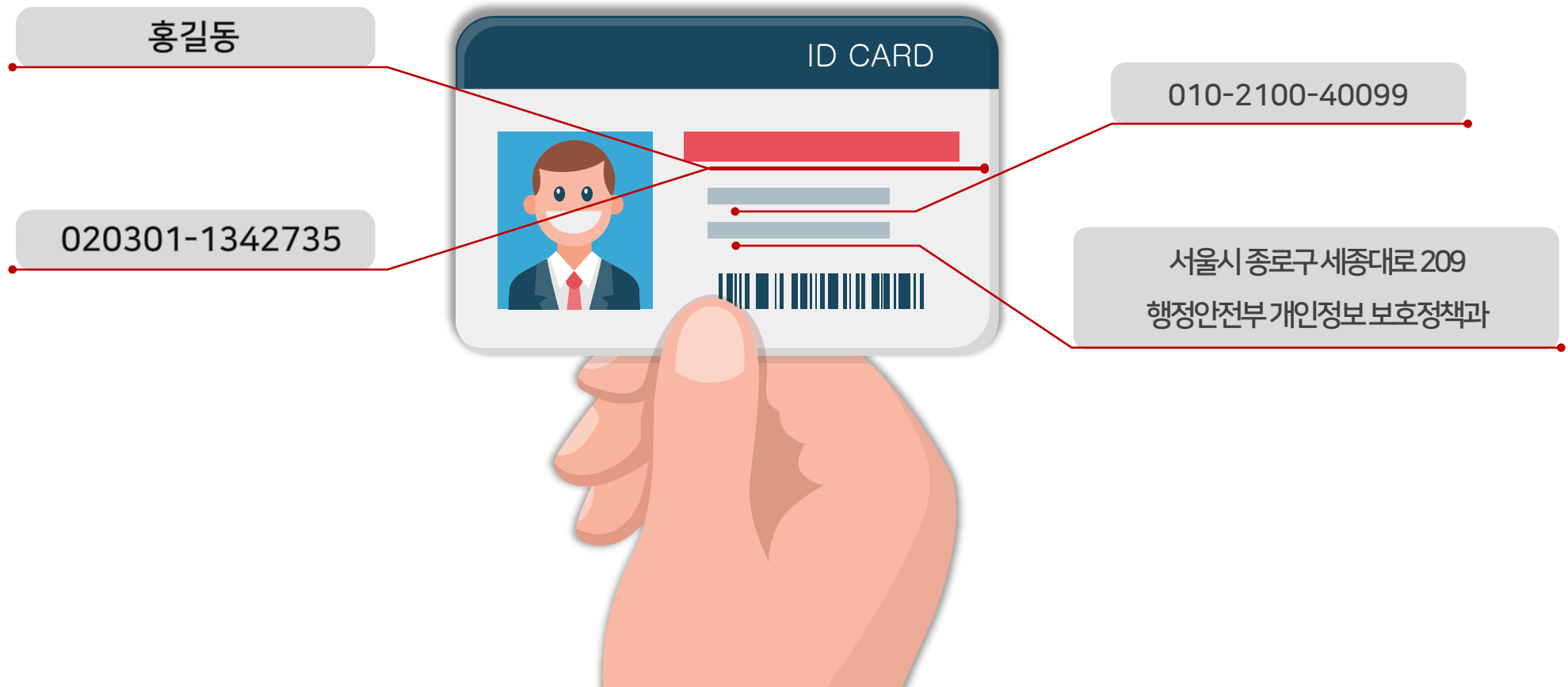
VI . 정보주체 권리 보장과 피해구제 등



I . 개인정보 보호의 중요성



개인정보란?



- 살아있는 개인을 알아볼 수 있는 정보
- 다른 정보와 쉽게 결합하여 특정 개인을 식별할 수 있는 정보

특정 개인을 식별할 수 있는 정보

주민번호, 영상정보, 지문 등



다른 정보와 결합하여 개인을 식별할 수 있는 정보

이름 + 전화번호
이름 + 주소
이름 + 주소 + 전화번호



개인정보인지 여부는 해당 정보가
다른 정보와 쉽게 결합하여
특정 개인을 식별할 수 있는지를
고려하여 판단하여야 함

개인정보의 종류

일반적 정보

- 주민등록번호
- 이름, 주소, 전화번호

정신적 정보

- 기호, 성향
- 신념, 사상

통신 위치 정보

- 통화, IP주소
- GPS 등

신체적 정보

- 신체정보
- 의료, 건강정보

사회적 정보

- 교육 정보
- 근로 정보
- 자격 정보

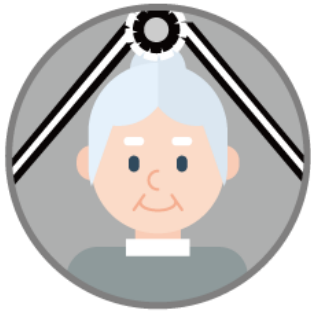
재산적 정보

- 개인
- 신용정보
- 부동산, 주식





1. '살아 있는' 개인에 관한 정보

구 분	내 용
개인정보	▶ '살아 있는' 자연인에 관한 정보 → 사망자의 정보라도 하더라도 유족과의 관계를 알 수 있는 정보는 유족과의 개인정보에 해당 
개인정보 불포함	▶ 사망했거나 실종신고 등 관계법령에 의해 사망한 것으로 간주된 자의 정보는 개인정보가 아님 

2. '개인에 관한' 정보

구 분	내 용
개인정보	▶ 법인 또는 단체에 관한 정보이면서 동시에 개인에 관한 정보 (예: 대표자·임원진·업무 담당자의 이름·주택주소 및 개인연락처, 사진 등) ▶ 해당 사물 등의 제조자 또는 소유자 등을 나타내는 정보 (아파트 소유자가 자연인인 경우, 아파트 주소가 특정 소유자 정보) ▶ SNS에 단체 사진(사진에 있는 인물 모두의 개인정보에 해당)
개인정보 불포함	▶ 법인 또는 단체에 관한 정보 (예: 법인 또는 단체 이름, 소재지 주소, 대표 연락처, 업무별 연락처) ▶ 개인사업자의 상호명, 사업장 주소, 전화번호 등 사업체의 운영관련 정보 ▶ 사물에 관한 정보 ▶ 특정 개인에 관한 정보임을 알아볼 수 없도록 통계적으로 변환된 정보

3. '정보'의 내용·형태 등은 제한 없음

구 분	내 용
개인정보	▶ 디지털 형태나, 수기 형태, 자동 처리나 수동 처리 등 그 형태 또는 처리방식과 관계없음 ▶ 정보주체와 관련되어 있으면 키, 나이, 몸무게 등 '객관적 사실'에 관한 정보, 그 사람에 대한 제3자의 의견 등 '주관적 평가'에 관한 정보, '사실' 이거나 '증명된 것' 이 아닌 부정확한 정보 또는 허위 정보

4. 개인을 '알아볼 수 있는' 정보

구 분	내 용
개인정보	▶ 해당 정보를 '처리하는 자'(향후 처리가 예정된 자도 포함) 의 입장에서 합리적으로 활용 될 가능성이 있는 수단을 고려하여 개인을 알아볼 수 있다면 개인정보에 해당 (예: 주민등록번호와 같은 고유식별정보)
개인정보 불포함	▶ 다른 정보 없이 그 자체만으로는 개인을 알아볼 수 없는 정보 (예: 생년월일)

5. 다른 정보와 '쉽게 결합하여' 개인을 알아볼 수 있는 정보

결합대상이 될 정보의 '입수 가능성'이 있어야 하고 '결합 가능성'이 높아야 함을 의미

구 분	내 용
입수 가능성	▶ 두 종 이상의 정보를 결합하기 위해서는 결합에 필요한 정보에 합법적으로 접근·입수 할 수 있어야 함 → 해킹 등 불법적인 방법으로 취득한 정보까지 포함하지 않음
결합 가능성	▶ 현재 기술 수준을 고려하여 비용이나 노력이 비합리적으로 수반되지 않아야 함

Q 휴대전화번호 뒤 4자리는
개인정보에 해당합니까?



A 휴대전화번호 뒷자리 4자만으로도 그 전화번호 사용자가 누구인지를 식별할 수 있는 경우가 있고, 특히 그 전화번호 사용자와 일정한 인적 관계를 맺어온 사람이라면 더욱 그러할 가능성이 높으며, 설령 휴대전화번호 뒷자리 4자만으로는 그 전화번호 사용자를 식별하지 못한다 하더라도 「그 뒷자리 번호 4자와 관련성이 있는 다른 정보(생일, 기념일, 집 전화번호, 가족 전화번호, 기존 통화내역 등)와 쉽게 결합하여 그 전화번호 사용자가 누구인지를 알아볼 수도 있다」고 하여 개인정보로 볼 수 있습니다. (대전지법 논산지원, 2013고단17 판결)

(출처: 행정안전부, 개인정보 보호 법령 및 지침·고시 해설, 2016.12)

참고

출근

(교통카드, CCTV)



이름, 계좌, 카드번호, 영상

오늘의 이슈?

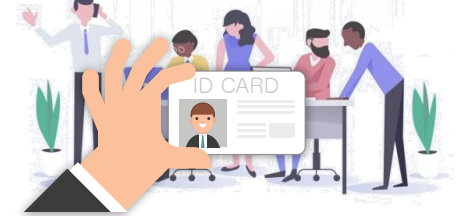
(SNS)



ID, PW, 사진, 동영상, 빅데이터

사무실 출입

(전자카드)



이름, 사번

일 하자!

(그룹웨어)



이름, 계좌, 카드번호, 영상

업체와 회의

(방문증 발급)



이름, 전화번호, 이메일

점심식사

(신용카드, 포인트카드)



이름, 신용카드, 연락처, 위치정보

주가가 올랐나?

(스마트폰)



ID, PW, 이름, 계좌

어머니 생신?!

(온라인 쇼핑)



ID, 신용카드, 주소, 연락처

병원에 잠깐

(의료기관)



건강보험번호, 이름, 병명, 진료기관

사랑하는 가족 곁으로

(아파트출입카드, CCTV)



이름, 동·호수, 연락처

퇴근 후 동창회 관리

(회원명부)



이름, 연락처, 전공, 졸업년도

모든 생활에
개인정보 연관

개 인

- 정신적 피해 및 보이스 피싱 등에 의한 금전적 손해
- 유괴 등 생명·신체를 위협하는 각종 범죄에 노출 우려 등

기 업

- 기업의 이미지 실추 및 소비자단체 등의 불매운동
- 다수 피해자에 대한 집단적 손해 배상 등으로 재정적 손실 등

국 가

- 정부·공공행정의 신뢰도 및 국가 브랜드 하락
- 프라이버시 라운드 대두에 따른 수출 애로 등



사 례

(개인) 개인정보 유출로 인한 정신적 피해

'개인정보 유출' 공익제보자 결국...경찰, 담당 공무원 입건

공익제보자가 자신의 개인정보가 유출된 것을 알고 끝내 스스로 목숨을 끊은 A씨의 사건과 관련해 경찰이 담당 공무원들을 입건했다. OO경찰서는 국민신문고 청원자 개인정보를 삭제하지 않고 외부로 유출한 혐의(개인정보 보호법 위반)로 OO교육청 직원 B씨(42)와 도교육청 산하 교원소청심사위원회 직원 C씨(37, 여)를 입건했다고 27일 밝혔다. 경찰은 청원자에게 협박성 문자메시지를 보낸 혐의(협박)로 전직 교사 P씨(60)도 입건했다.

(출처: 연합뉴스TV, 2018.12.26.)



(사진: 연합뉴스)

사 례

(개인) 이미지 실추 및 생명 위해 우려

OO센터PC 해킹...탈북민 997명 개인정보 유출

탈북민의 성명·생년월일·주소 담김 파일 유출!

이번 해킹을 주도한 해커의 신원과 목표가 아직 밝혀진 게 없는 상황이라 탈북민들은 불안감을 감추지 못했다
탈북민들 개인정보 유출에 잠 못 드는 이유... “개인정보 유출? 북한에 있는 가족들 신변이 더 위험하다.”

(출처: 한겨레, 2018.12.28.)



(사진: 연합뉴스)

사 례

(개인) 개인정보 도용 피해

2015년 도박 혐의로 검거된 A씨는 1984년 절취한 B씨의 신분증과 학생증으로 B씨의 신분을 도용하여 살아왔으며, 1987년 항정신성의약품위반죄로 징역 1년, 2015년 즉결심판 청구 되었음, 이에 B씨는 신분도용의 피해를 우려하여 주민등록번호 변경결정 청구, 이에 주민등록번호변경 심의위원회는 변경결정 신청을 받아들임

(출처: 행정안전부, 주민등록번호 변경결정 사례집, 2018.12.18.)

사 례

(기업) 개인정보 유출로 인한 손해배상 및 이미지 실추

法 “OO마트, 개인정보 유출 고객들에 배상하라”

서울중앙지법 민사31부는 2018년 1월 18일
개인정보 유출 피해 고객 1067명이 OO마트 를
상대로 손해배상을 청구한 소송에서
“피해자들에게 1인당 5만~30만원씩 총
8365만원을 지급하라”고 판결했다.



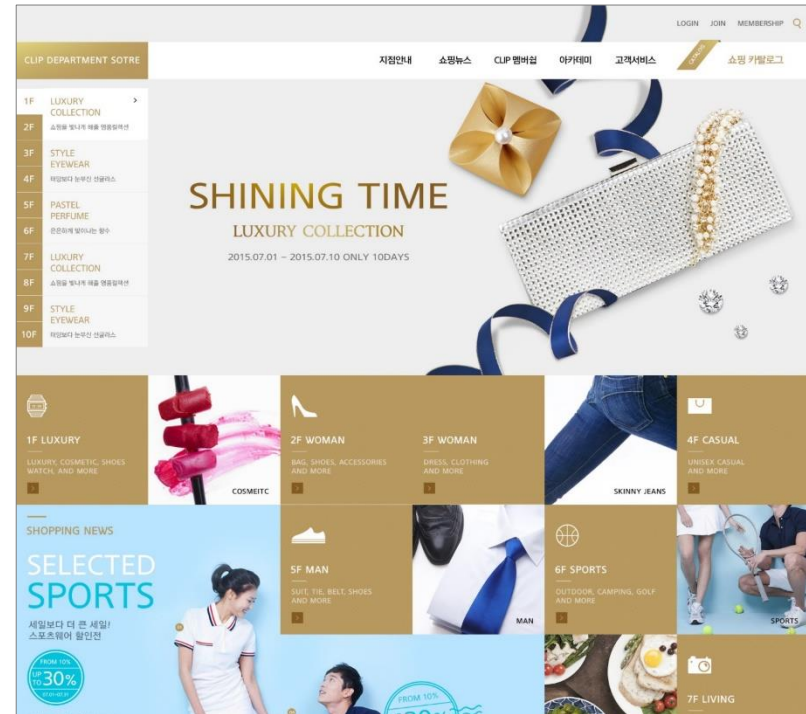
(출처: 조선닷컴, 2018.1.18.)

사 례

(기업) 개인정보 유출로 인한 손해배상 및 이미지 실추

'개인정보 유출' OO 인터넷 쇼핑몰, 45억 과징금

2016년 개인정보 유출 사건으로
방송통신위원회로부터
45억원 상당 과징금을 부과 받은 OO 인터넷
쇼핑몰이 처분이 부당하다며 소송을 제기했지만
받아들여지지 않았다.



(출처: 중앙일보, 2018.7.5.)

국 가

- 개인정보 보호를 위한 시책 수립·시행
- 정보주체 권리 보호를 위한 법령 정비 등
- 개인정보 보호 자율규제 촉진·지원

기 업

- 개인정보 보호 조직 구성 및 정책·지침 수립
- 정보주체의 개인정보 보호를 위한 안전성 확보 조치 등 법규 준수
- 개인정보취급자등에 대한 정기적인 교육 및 훈련

개 인

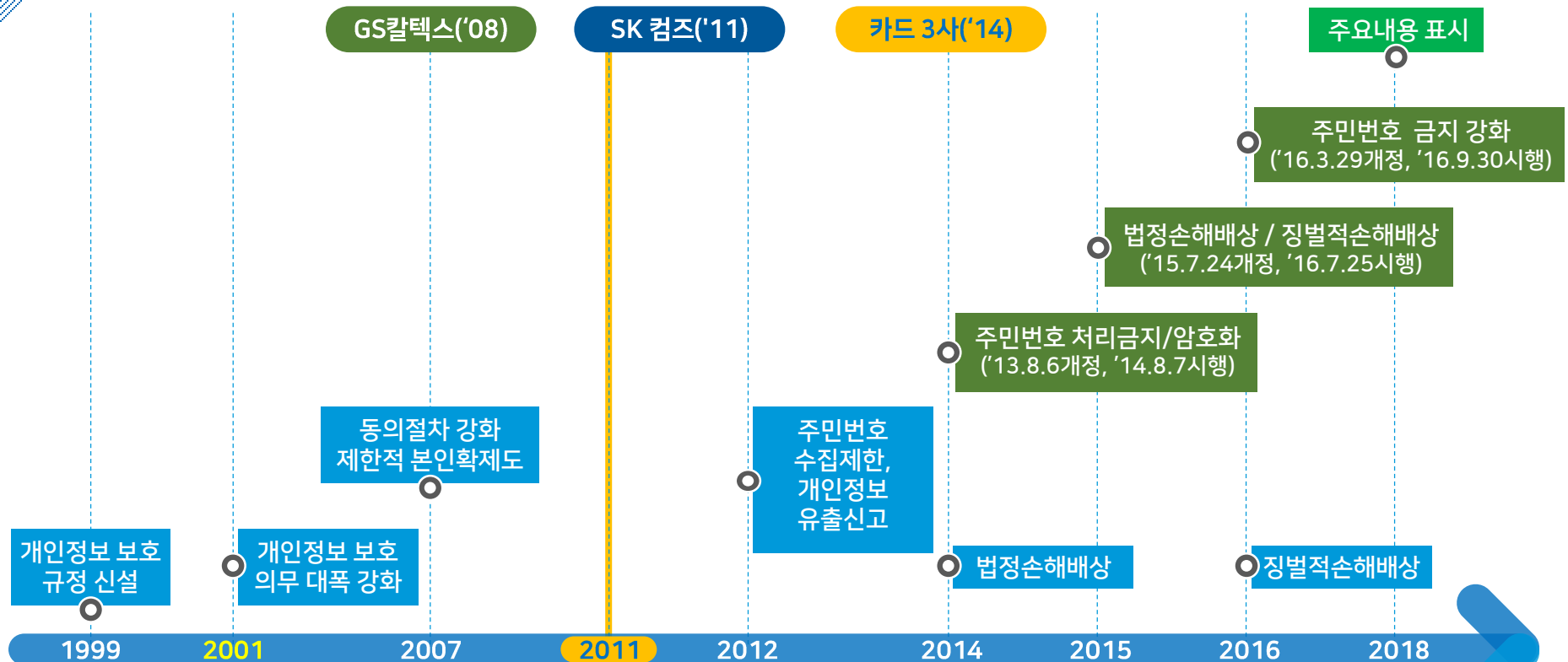
- 개인정보 보호의 중요성 및 피해 구제방안 인식
- 생활 속에서 개인정보 보호 실천



개인정보 자기결정권

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

개인정보 보호법 관계 법령 변천사



정보통신법('01)

일반법 역할

개인정보 보호법('11.3.29)

일반법

정보통신망이용촉진등에 관한법률('99)

전산망보급확장과이용촉진에관한법률('87)



개인정보 보호법은 개인정보 보호 분야의 일반법

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

타 법률에 특별한 규정이 있는 경우

- » 해당 법률의 규정을 우선 적용
 - ※ 정보통신망법, 신용정보법, 전자금융거래법, 의료법 등



**Q 「개인정보 보호법」
「정보통신망법」 「신용정보 보호법」 중
어느 법이 우선 적용되나요?**



A

개인정보 수집에 대한 동의를 받을 때 「정보통신망법」과 「신용정보보호법」은 각각 별도의 규정이 있으므로 이에 대하여는 「개인정보 보호법」보다 우선하여 적용됩니다.

그러나 「정보통신망법」과 「신용정보보호법」등에는 영상정보처리기기 설치운영 제한, 분쟁 조정, 단체소송 등의 규정이 없으므로 이에 대하여는 「개인정보 보호법」이 우선하여 적용됩니다.

참 고

「개인정보 보호법」은 모든 국민의 개인정보를 보호대상으로 하고

「정보통신망법」은 정보통신망서비스 제공자의 이용자, 즉 고객이 개인정보를 보호대상으로 하고

「신용정보보호법」은 금융기관 고객의 개인신용정보를 보호대상으로 함

II. 총 칙 (개인정보 보호법 제1장)



개인정보 보호 원칙 및 정책

- 개인정보 보호 원칙
- 정보주체의 권리
- 개인정보 보호 정책 추진체계



개인정보의 처리 단계별 의무

- 개인정보 처리단계별 규정
 - 개인정보 수집, 이용, 제공, 파기
 - 단계별 준수해야 할 사항
- 개인정보 처리제한
 - 주민등록번호, 민감정보 처리 제한

개인정보의 안전한 관리

- 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

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

개인정보보호법의 구성

» 제1장 총칙

목적, 정의, 개인정보 보호원칙, 다른 법률과의 관계 등

» 제2장 개인정보 보호정책의 수립 등

개인정보 보호위원회, 기본계획·시행계획 수립, 개인정보 보호지침, 자율규제촉진 등

» 제3장 개인정보의 처리

수집·이용·제공 등 처리기준, 민감정보·고유식별정보 제한, 영상정보처리기기 제한 등

» 제4장 개인정보의 안전한 관리

안전조치의무, 개인정보파일 등록·공개, 개인정보영향평가, 유출통지제도 등

» 제5장 정보주체의 권리 보장

열람요구권, 정정·삭제요구권, 처리정지요구권, 권리행사방법 및 절차, 손해배상책임 등

» 제6장 개인정보분쟁조정위원회

분쟁조정위원회 설치·구성, 분쟁조정의 신청방법·절차·효력, 집단분쟁조정제도 등

» 제7장 개인정보 단체소송

단체소송 대상, 소송허가요건, 확정판결의 효력 등

» 제8장 보칙

적용제외, 금지행위, 침해사실신고, 시정조치 등

» 제9장 벌칙

벌칙, 과태료 및 양벌 규정 등

» 부칙

시행일, 경과조치, 다른 법률의 개정 등

개인정보

- ▶ 성명, 주민등록번호 및 영상 등을 통하여 살아있는 개인을 알아볼 수 있는 정보
- ▶ 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보
※ 개인정보 보호법은 정보통신망법과는 달리 이용자뿐 아니라 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



참고

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 지휘 · 감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등

개인정보 처리시스템

- ▶ 데이터베이스 시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 응용시스템

영상정보 처리기기

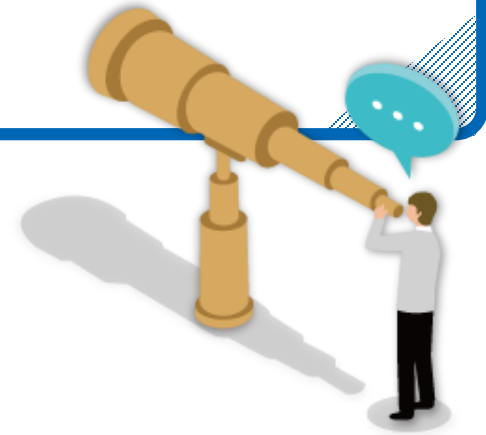
- ▶ 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치



- 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》 가능한 경우 익명 처리
- 8》 개인정보처리자의 책임 준수, 정보주체의 신뢰성 확보



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

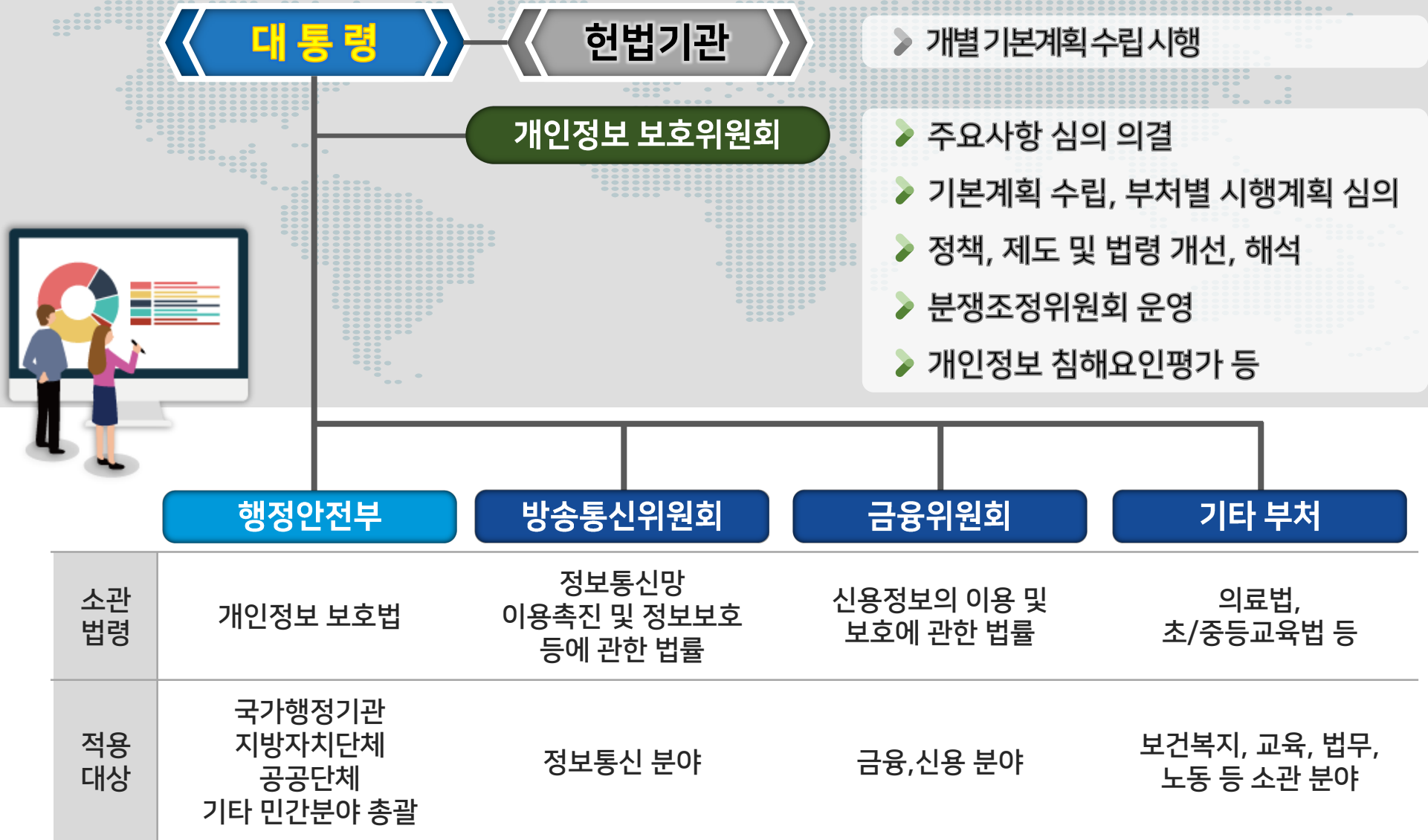


III. 개인정보 보호 정책의 수립 등

(개인정보 보호법 제2장)



개인정보 보호 추진체계



출범 및 구성

- ▶ 대통령 소속의 합의제 행정기관으로 2011년 출범
- ▶ 위원 15명(위원장 1명, 상임위원 1명, 대통령 위촉 5명, 국회 선출 5명, 대법원 지명 5명)

개인정보 보호위원회 안건 처리 현황

구분		안전 처리 건수						
		'11~'12년	'13년	'14년	'15년	'16년	'17년	계
합계(법 제8조 제1항 각호)		22	22	39	37	129	701	950
개인정보 침해요인 평가(1호)	침해요인 평가	-	-	-	-	64	304	368
	평가대상 여부 심사	-	-	-	-	32	353	385
기본계획·시행계획(1호의2)		2	2	1	1	2	1	9
정책·제도·법령의 개선(2호)		6	7	7	4	-	14	38
공공기관 간 의견 조정(3호)		(1)	(3)	(5)	(4)	(5)	(5)	(23)
법령 해석·운용(4호)		2	5	12	15	15	14	63
목적 외 이용·제3자 제공(5호)		4	6	6	6	5	6	33
행안부장관 요청 심의·의결(6, 7, 9호)		-	-	10	7	7	1	25
공공기관 시정권고(8호)		-	-	-	1	-	-	1
연차보고서(10호)		1	1	1	1	1	1	6
위원 2인 이상, 타법, 기타(11, 12호)		7	1	2	2	3	7	22

※ 목적 외 이용·제3자 제공(5호) 건 중 공공기관 간 의견 조정에 관한 건은 팔호(3호)로 기재

(출처: 개인정보 보호위원회, 2018 연차보고서)

침해요인 평가 제도란?

- ▶ 법령 제·개정시 개인정보 침해요인이 존재하는지를 평가하여 소관기관의 장에게 보완할 것을 권고하는 제도

침해요인 평가 내용

- ▶ 개인정보 처리의 필요성
- ▶ 개인정보 주체의 권리보장의 적정성
- ▶ 개인정보 관리의 안전성
- ▶ 그 밖에 침해요인 평가에 필요한 사항



개인정보 보호 기본계획 및 시행계획 (제9,10조)

구 분	기 본 계 획	시 행 계 획
작성주체	▶ 개인정보 보호위원회와 관계 중앙행정기관	▶ 관계 중앙행정기관 ※ 18년 12월 기준 : 18부 4처 17청, 6개 위원회*, 국정원, 감사원, 국무조정실 등 총 48개
작성주기	▶ 3년	▶ 1년
작성절차	▶ 기본계획 시작 해의 전전년도 12월 31일까지 수립	▶ 시행계획 작성지침 수립 · 통보(전년도 12월) : 개인정보 보호위원회 → 각 중앙행정기관 ▶ 중앙행정기관별 시행계획 작성·제출(해당년도 2월) : 각 중앙행정기관 → 개인정보 보호위원회 ▶ 시행계획 심의·의결 및 결과 통보(해당년도 4월) : 개인정보 보호위원회 → 각 중앙행정기관
작성내용	▶ 기본목표와 추진 방향 제시 : 법제도 개선방안, 개인정보 침해방지 대책, 개인정보 보호 교육방안 등	▶ 연간 세부 시행계획

개인정보처리자가 개인정보를 안전하게 이용·보호하도록 하기 위하여
개인정보 처리 절차와 방법에 따른 보호조치를 등에 관한 사항을 담은 지침

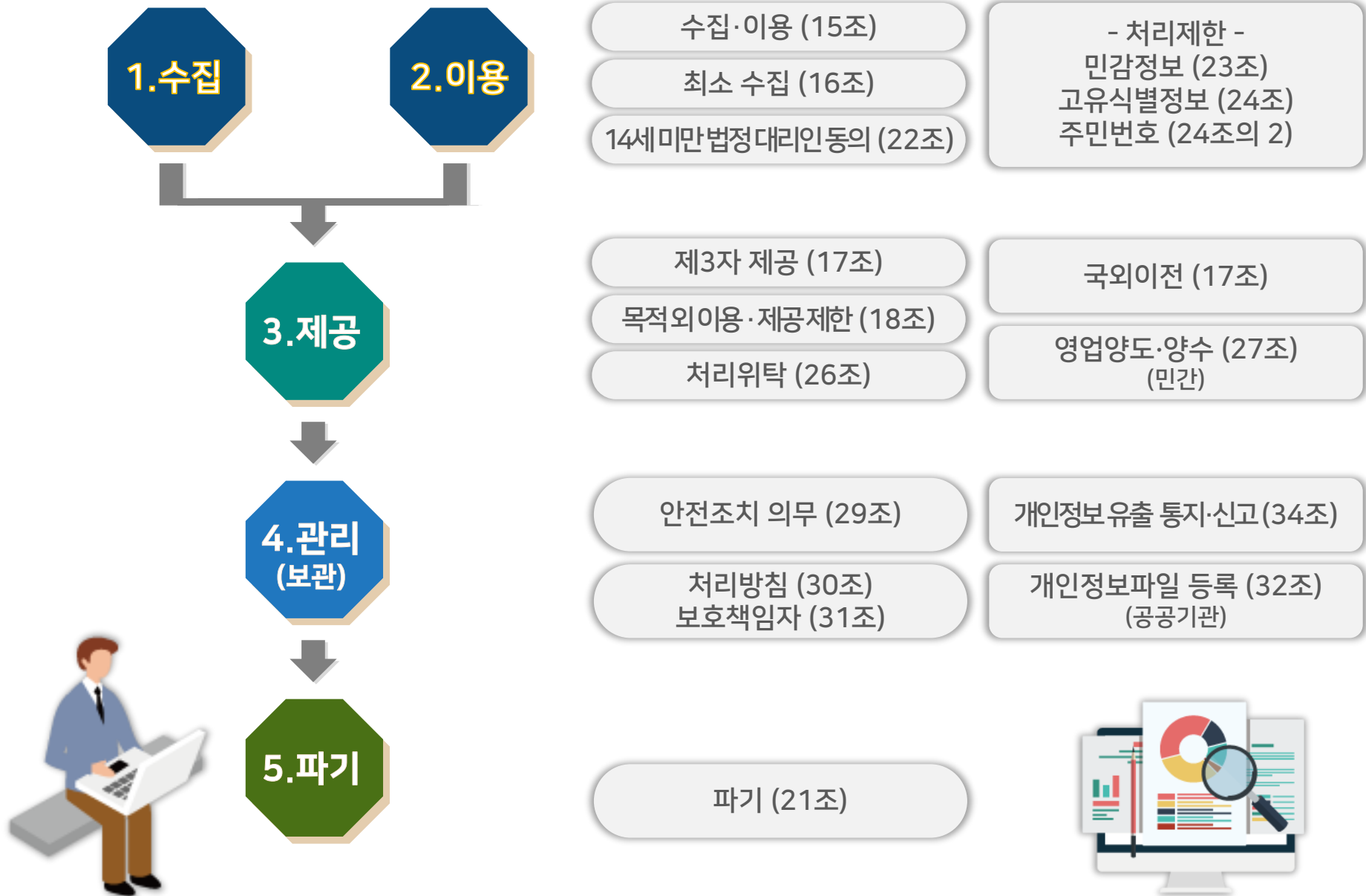
구 분	표준 개인정보 보호지침	소관 분야별 개인정보 보호지침
작성주체	▶ 행정안전부	▶ 중앙행정기관 또는 헌법기관
내 용	① 개인정보 처리 기준 - 개인정보 수집·이용·제공 및 파기하는 경우에 법률에서 정한 요건이 적합한지 여부를 판단할 수 있는 기준과 사례 ② 개인정보 침해 유형 - 개인정보처리자의 작위 또는 부작위가 개인정보 침해에 해당 되는지 여부 판단기준과 사례 ③ 개인정보 침해예방 - 개인정보 권리 침해 예방을 위해 개인정보처리자가 지켜야 할 보호·이행 조치	

IV. 개인정보의 처리

(개인정보 보호법 제3장)



개인정보 처리단계별 보호조치



※ 민감정보, 고유식별정보는 제15조, 제17조, 제18조 해당 없음!

1. 정보주체의 동의를 받은 경우

※ 동의 받을 때 고지 의무 사항

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

2. 법률의 특별한 규정, 법령상 의무 준수를 위해 불가피한 경우

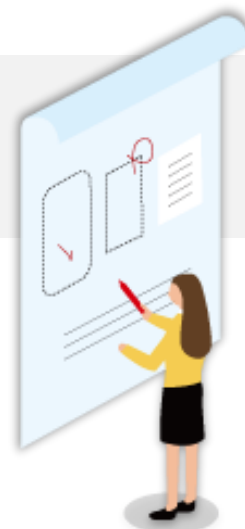
3. 공공기관이 법령 등에서 정한 소관업무를 위해 불가피한 경우

4. 정보주체와의 계약 체결이행에 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

※ 민감정보, 고유식별정보는 제15조, 제17조, 제18조 해당 없음!

1. 필요 최소한 개인정보 수집

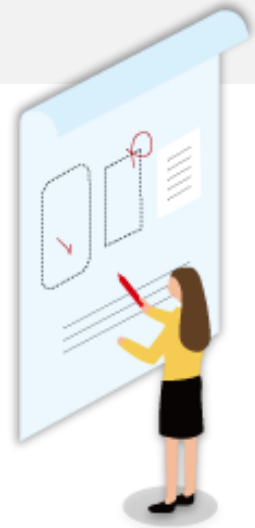
※ 정보주체의 동의를 받거나 법령의 처리 근거 또는 계약의 체결·이행 등을 위해 불가피하게 개인정보를 수집하는 경우에도 처리 목적 달성에 필요한 최소한의 개인정보만을 수집

2. 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담

3. 필요 최소한의 정보 외의 개인정보 수집에는 동의 거부 가능

4. 최소한의 개인정보 이외의 개인정보 수집에 동의하지 않는다는

이유로 재화 등 제공 거부 금지



위반 시 ➡ 3천만원 이하의 과태료

Q 학원에서 수강생의 성명, 성별, 생년월일, 지역, 출신학교, 휴대전화번호 등을 적으라고 하는데, 과도한 수집이 아닌가요?



A 학원은「학원의 설립·운영 및 과외교습에 관한 법률 시행규칙」제16조에 따라 수강생대장을 기록·유지하여야 합니다.

수강생대장에는 등록번호, 성명, 생년월일, 주소, 전화번호, 입원 연월일, 퇴원 연월일 등을 기재하도록 하고 있습니다.

그 외, 성별, 지역, 출신학교는 법령에서 정한 항목이 아니므로 학원 운영을 위하여 반드시 필요한 경우가 아니라면 수집하지 말아야 합니다.

(출처: 한국인터넷진흥원, 개인정보 보호 상담 사례집, 2017.1)

※ 민감정보, 고유식별정보는 제15조, 제17조, 제18조 해당 없음!

1. 정보주체의 동의를 받은 경우

※ 동의 받을 때 고지 의무 사항

- 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 범위내에서 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

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 직제·직제규칙, 개별 조직법 등에서 정하고 있는 소관 사무
- 「주민등록법」, 「의료법」, 「국민건강보험법」 등 개별 법에서 정하고 있는 소관 사무



※ 민감정보, 고유식별정보는 제15조, 제17조, 제18조 해당 없음!

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

1. 정보주체의 별도 동의를 받은 경우
2. 다른 법률의 특별한 규정
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 개인정보 보호위원회의 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

사례

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

사례

목적 외 이용 위반 사례

- 사전 동의절차 없이 교육 등 마케팅 홍보자료를 이메일 발송한 경우
- 세무 공무원이 자신과 채권채무 관계로 소송 중인 사람의 납세정보를 조회하여 소송에 활용한 경우
- 상품배송을 목적으로 수집한 개인정보를 동의 받지 않고 상품·서비스의 홍보에 이용
- 인물검색 포털 등에 공개된 개인정보를 활용하여 마케팅에 이용하는 행위

목적 외 제공 위반 사례

- 주민센터 복지카드 담당 공무원이 복지카드 신청자의 개인정보를 정보주체의 동의 없이 사설학습지 회사에 제공
- 홈쇼핑 회사가 주문상품을 배달하기 위해 수집한 고객정보를 정보주체의 동의 없이 계열 콘도미니엄사에 제공하여 콘도미니엄 판매용 홍보자료 발송에 활용
- 자치단체가 운영하는 쇼핑몰의 회원에게 동의 없이 자치단체장의 시정 현황 홍보
- 선거인명부를 법적 근거없이 지역내 후보자 선거사무소에 제공

제 공 자

개인정보를 제공받는 자에게
이용목적, 이용방법 그 외 필요
사항에 대한 제한 및 개인정보
안전성 확보 조치 마련 요청

요 청



제 공 받 는 자

개인정보 안전성
확보 조치 이행

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



■ 개인정보 보호법 시행규칙 제3조 [별지 제1호 서식]

개인정보 또는 개인정보파일 명칭			
이용 또는 제공 구분	[] 목적 외 이용	[] 제 3자 제공	
목적 외 이용기관의 명칭 (목적 외 이용의 경우)		담당자	소속 :
			성명 :
			전화번호 :
제공받는 기관의 명칭 (제3자 제공의 경우)		담당자	소속 :
			성명 :
			전화번호 :
이용하거나 제공한 날짜, 주기 또는 기간			
이용하거나 제공한 형태			
이용 또는 제공의 법적 근거			
이용 목적 또는 제공받는 목적			
이용하거나 제공한 개인정보의 항목			
「개인정보 보호법」 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용			

▶ 정보주체 이외로부터 수집한 개인정보를 처리할 때, 정보주체의 요구가 있으면 즉시 다음의 사항을 알려야 함

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

▶ 법제17조제1항에 따라 정보주체의 동의를 받아 제3자로부터 개인정보를 제공받은 경우 정보주체에게 수집 출처, 처리 목적, 처리 정지 요구가 가능함을 고지하여야 함

※ 단, 정보주체에게 알릴 수 있는 개인정보가 없다면 예외 가능

▶ 고지대상

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

▶ 고지방법

- 서면, 전화, 문자전송, 전자우편 등 방법, 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

Q

대학 홈페이지 등에 공개된
교수 등의 개인정보를 이용하여 인물DB를
만드는 경우 고려해야 할 사항은?



A

이른바 '공개된 개인 정보'는 당초 공개된 목적 내에서만 이용할 수 있습니다.

예컨대 동창회 명부라면 해당 회원들의 상호 연락 및 친목 도모에만 이용될 수 있으며,
회원의 동의를 얻지 않은 마케팅 행위 등에는 이용할 수 없습니다.

대학 홈페이지 등에 공개된 교수의 개인정보는 학술연구와 자문, 저술활동, 기고 등에 쓰일 것을
전제하고 있다고 보이므로 정보주체에게 개인정보 수집에 대한 동의를 받을 필요는 없으나,
만약 정보주체가 요구한 경우에는 즉시 개인정보의 수집 출처, 처리 목적, 개인정보 처리의 정지를
요청할 권리가 있다는 사실을 고지하여야 합니다.

➤ 보유기간의 경과, 처리목적 달성 등 개인정보가 불필요하게 되었을 때 지체 없이(5일 이내) 파기, 다만 다른 법령에 규정이 있으면 보존 가능

➤ 개인정보 파기할 때에는 **복구 · 재생되지 않도록** 조치

➤ 다른 법령에 따라 보존하여야 하는 경우 다른 개인정보와 분리하여 저장·관리



파 기 방 법

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

파 기 절 차

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

- ▶ 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 개인정보**와 정보주체의 **동의를 필요한 개인정보**를 구분
 - 제15조 제1항 제1호, 제17조 제1항 제1호, 제23조 제1항 제1호 및 제24조 제1항 제1호에서 정보주체의 동의 필요
 - 동의 없이 처리 가능한 개인정보라는 입증책임은 개인정보처리자에게 있음
- ▶ 홍보나 마케팅 등의 이유로 개인정보처리 동의를 받으려 할 때는 **정보주체가 이를 명확하게 인지하고 동의**해야 함
- ▶ 선택적으로 동의할 수 있는 사항을 동의하지 않는다는 이유로 재화 또는 서비스의 제공을 거부해서는 안 됨
- ▶ **만 14세 미만** 아동의 개인정보를 처리하려면 **법정대리인의 동의**를 받아야 함
 - 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 해당 아동으로부터 직접 수집할 수 있음



동의서에 명확히 표시하여야 하는 사항

- ▶ 재화나 서비스의 홍보 및 판매 권유, 기타 이와 관련된 목적으로 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실
- ▶ 개인정보 중 다음 각 목의 사항
-민감정보, 여권번호, 운전면허의 면허번호 및 외국인등록번호
- ▶ 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적
- ▶ 개인정보의 보유 및 이용 기간



★ 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

사례

- ▶ A사는 프렌차이즈 외식 업체이다. 홈페이지를 이용하여 이벤트, 광고, 식당 예약을 위하여 정보주체에게 개인정보를 수집하고 있다. 이 과정에서 14세 미만의 정보주체의 개인정보를 수집할 때 법정대리인의 동의를 받아야 하는데, 법정대리인의 동의를 받지 않았다.

현장점검 사례

성명(*)	
아이디(*)	중복확인
비밀번호	14세 미만 정보주체의 개인정보를 수집 시 법정 대리인의 동의를 받지 않음.
비밀번호 확인(*)	
이메일(*)	@ 직접입력 ▼ 중복확인
주소(*)	시도 ▼ 시군구 ▼
휴대전화(*)	010 ▼ - - 인증번호 발송 인증번호 입력
전화번호	02 ▼ - -
이메일 수신동의	이메일을 이용한 마케팅 활용에 동의하시겠습니까? (선택) ○ 수신동의 ● 동의하지 않음
SMS 수신동의	SMS를 이용한 마케팅 활용에 동의하시겠습니까? (선택) ○ 수신동의 ● 동의하지 않음

법정대리인 동의 내용 사인
필수 양식 내용 기재 의무

위반 사항

이 사례에서 A사는 홈페이지(온라인)에서 14세 미만의 개인정보를 수집할 때에는 법정 대리인의 동의를 받아야 하는데, 동의를 받지 않았으므로 개인정보 보호법 제22조제6항 위반에 해당한다.

위반에 따른 벌칙

위반행위	벌칙
법정대리인의 동의를 받지 아니한 자 (제22조제6항)	5천만 원 이하 과태료 (제75조제1항제2호)

행정 처분 결과

14세 미만 개인정보 수집 절차 개선 관련 시정조치
- 14세 미만의 정보주체에게 개인정보를 처리할 때 해당 정보주체의 법정대리인의 동의를 받아야 한다.

처분 내용

5,000만 원 이하 과태료

개인정보처리자 시정조치 사항

법정대리인의 휴대폰 인증을 통해 법정대리인 동의 획득

법정대리인 휴대전화(*)	010 ▼ - - 인증번호 발송 인증번호 입력
------------------	---

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
00군부대	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)

“ 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

분실·도난·유출·위조·변조·훼손되지 않도록
안전성 확보조치 의무

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



조사대상

- ▶ 공공기관
- ▶ 5만 명 이상 정보주체의 고유식별정보를 처리하는 자

조사주기

- ▶ 2년마다 1회 이상

조사방법

- ▶ 고유식별정보 보유현황 및 안전성 확보조치 자체점검 결과를 개인정보 보호 종합포털(privacy.go.kr)에 등록

수행기관

- ▶ 한국인터넷진흥원 또는 행정안전부장관이 고시하는 기관



주민등록번호는 정보주체의 동의를 받아도 처리 불가!

다음의 어느 하나에 해당하는 경우에만 주민등록번호 처리 가능

- ▶ 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
- ▶ 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 보호
- ▶ 위의 사항에 준하는 경우로서 행정안전부령으로 정하는 경우

인터넷으로 회원 가입 시 본인확인이 필요한 경우, 주민번호 대체수단을 제공하여야 함

- ▶ (예) I - PIN, 휴대폰, 공인인증서, 전자서명 등



Q

공공기관이 입사지원서에 주민등록번호를 기재하도록 요구하는데 적법한 것인가요?



A

채용지원 단계에서는 주민등록번호를 수집할 수 없습니다.

다만 채용이 결정된 후 법령을 근거로 주민등록 처리를 요구하는 경우 수집이 가능합니다.

입사지원서 접수, 필기시험, 면접 등 채용 전형과정에서는 해당 전형에 필요한 최소한의 개인정보만 수집하여야 합니다. 특히 주민등록번호는 법령에 처리 근거 등의 예외적인 사유가 존재하지 않은 한 원칙적으로 수집이 금지되므로 채용 전형 과정에서는 주민등록번호를 처리할 수 없습니다.

다만 채용결정 후 사용자가 근로자 의무 보험 또는 국민연금 등을 처리해야 할 법령상의 의무 이행을 위해 관련 법률에 따라 제공해야 하므로 수집가능하고, 이때는 근로자의 동의는 필요하지 않습니다.

▶ 처리위탁은 문서에 의해서 해야 함 (제1항)

문서에 포함될 내용

- ① 위탁업무 수행목적 외 개인정보의 처리 금지
- ② 개인정보의 기술적 · 관리적 보호조치
- ③ 위탁업무의 목적 및 범위
- ④ 재위탁 제한
- ⑤ 개인정보에 대한 접근 제한 등 안전성 확보 조치
- ⑥ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등의 감독
- ⑦ 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등의 책임



▶ 위탁하는 업무 내용, 수탁자를 인터넷 홈페이지에 공개

▶ 홍보, 마케팅 업무 위탁시 업무 내용과 수탁자를 정보주체에게 고지

▶ 수탁자가 개인정보를 안전하게 관리할 수 있도록 수탁자 교육, 감독

▶ 수탁자의 이 법 위반으로 발생한 손해배상책임은 위탁자에게 있음

개인정보 처리 위·수탁 단계별 주요 조치사항

단 계	주 요 내 용
계약전	▶ 위험도 분석 등 예방조치를 통한 개인정보 유출 위험 최소화 - 위·수탁하는 개인정보의 가치, 유출 사고 시 정보주체가 입는 피해 정도 등 개인정보 위험 평가를 통한 위·수탁 대상 업무 구분 - 수탁자로 인한 개인정보 위험 최소화를 위하여 관리적, 기술적, 물리적 관점에서 수탁자 개인정보 보호 역량 종합 평가 - 위·수탁 업무 수행에 필요한 최소한의 개인정보 목록을 위탁자와 수탁자 간 사전 협의하여 개인정보 처리 범위 및 책임 소재 명확화 - 개인정보 위험의 체계적·지속적 관리를 위한 위·수탁자 주요 협의 사항 문서 작성 (「개인정보 보호법」 제26조 제1항)

(출처: 행정안전부, 개인정보 처리 위 수탁 안내서, 2018.6)

개인정보 처리 위·수탁 단계별 주요 조치사항

단 계	주요 내용				
업무 수행 중	▶ 개인정보 위·수탁에 따른 위탁자 및 수탁자의 주요 의무 사항 명확화 <table border="1"> <thead> <tr> <th>위탁자</th><th>수탁자</th></tr> </thead> <tbody> <tr> <td> -수탁자의 개인정보 관리체계,기술적·물리적 보호 조치의 적절성 여부 감독 ※자료제출요구,현장방문,시스템을 통한 원격 점검 등 다양한 수단 활용 가능 -수탁자 대상 개인정보 보호 교육 ※(원칙)위탁자 직접 교육 (예외) 외부 전문가, 수탁자 자체 교육 후 증빙 확인 </td><td> -「개인정보 보호법」제26조 제7항에 의한 의무 이행 ※특히법제29조의 안전조치 의무 적용 -수탁자 고의 또는 과실로 정보주체에 피해를 입힌 경우 손해배상 책임 -개인정보 처리 재위탁은 위·수탁 문서에 근거해야 함 </td></tr> </tbody> </table>	위탁자	수탁자	-수탁자의 개인정보 관리체계,기술적·물리적 보호 조치의 적절성 여부 감독 ※자료제출요구,현장방문,시스템을 통한 원격 점검 등 다양한 수단 활용 가능 -수탁자 대상 개인정보 보호 교육 ※(원칙)위탁자 직접 교육 (예외) 외부 전문가, 수탁자 자체 교육 후 증빙 확인	-「개인정보 보호법」제26조 제7항에 의한 의무 이행 ※특히법제29조의 안전조치 의무 적용 -수탁자 고의 또는 과실로 정보주체에 피해를 입힌 경우 손해배상 책임 -개인정보 처리 재위탁은 위·수탁 문서에 근거해야 함
위탁자	수탁자				
-수탁자의 개인정보 관리체계,기술적·물리적 보호 조치의 적절성 여부 감독 ※자료제출요구,현장방문,시스템을 통한 원격 점검 등 다양한 수단 활용 가능 -수탁자 대상 개인정보 보호 교육 ※(원칙)위탁자 직접 교육 (예외) 외부 전문가, 수탁자 자체 교육 후 증빙 확인	-「개인정보 보호법」제26조 제7항에 의한 의무 이행 ※특히법제29조의 안전조치 의무 적용 -수탁자 고의 또는 과실로 정보주체에 피해를 입힌 경우 손해배상 책임 -개인정보 처리 재위탁은 위·수탁 문서에 근거해야 함				
업무 종료 후	▶ 위·수탁 종료 시 지체 없는 개인정보 파기(반환)를 통한 개인정보 불법처리·유통 방지 -위·수탁 문서에 명시된 개인정보 처리 기간이 종료되거나, 사업 중이라도 개인정보 처리 목적이 달성된 경우 지체 없는 파기(5일)가 원칙 -수탁자는 위탁자 요청 시 개인정보를 즉시 반환하며, 이 경우 개인정보의 무결성 및 완전성을 보장 -위탁자는 수탁자의 개인정보 파기 여부 확인 후 증빙 자료를 넘겨야 함				

(출처: 행정안전부, 개인정보 처리 위 수탁 안내서, 2018.6)

Q

온라인 쇼핑몰에서 회원가입 신청을 받을 때
개인정보 제공 및 처리 위탁에 대한 동의를
한꺼번에 받아도 되나요?



A

개인정보제공 및 처리위탁에 대한 동의는 각각 별도로 받아야 합니다.

※ 공공기관, 정보통신서비스제공자 이외의 기업은 위탁에 대한 동의를 받을 필요는 없습니다.

참 고

온라인 사이트를 운영하는 정보통신서비스 제공자는 경품 이벤트를 위해 개인정보를 수집하는 경우 개인정보를 수집하는 경우 개인정보 수집·이용 동의 예외사유에 해당하는 경우를 제외하고는 이용자에 대해 개인정보 수집·이용에 대한 동의를 받아야 합니다.

<개인정보 수집·이용 동의 예외사유>

- 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우
- 정보통신서비스의 제공에 따른 요금정산을 위해 필요한 경우
- 법률에 특별한 규정이 있는 경우

또한 경품 이벤트 진행과정에서 개인정보 처리를 위탁하거나 개인정보의 제3자 제공이 발생하면 처리 위탁 또는 제공에 대해 이용자의 동의를 받아야 합니다.

V. 개인정보의 안전한 관리

(개인정보 보호법 제4장)



개인정보가 분실·도난·유출·위조·변조·훼손되지 않도록 안전성 확보 조치를 해야 함

개인정보의 안전성 확보조치 기준 (행정안전부 고시)

- 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 잠금 장치의 설치 등 물리적 조치

개인정보 처리 방침의 주요 내용

1. 개인정보의 **처리 목적**
2. 처리하는 개인정보의 **항목**
3. 개인정보의 **처리 및 보유기간**
4. 개인정보의 **제3자 제공**에 관한 사항 (해당하는 경우에만 정한다)
5. 개인정보의 **파기**에 관한 사항
6. 개인정보 처리 위탁자 담당자 연락처, 위탁자의 관리 현황 점검 결과 등 개인정보처리 **위탁에 관한 사항** (해당하는 경우에만 정한다)
7. 영 제30조1항에 따른 개인정보의 **안전성 확보조치**에 관한 사항
8. 개인정보의 열람,정정·삭제,처리정지 요구권 등 **정보주체의 권리·의무 및 그 행사방법**에 관한 사항
9. 개인정보의 **처리방침의 변경**에 관한 사항
10. **개인정보 보호책임자**에 관한 사항
11. 개인정보의 열람청구를 **접수·처리하는 부서**
12. 정보주체의 권익침해에 대한 **구제방법**



개인정보 보호책임자

역 할

개인정보의 처리에 관한 업무를 총괄, 책임

업 무

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오·남용 방지를 위한 내부통제시스템 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 개인정보 처리방침의 수립·변경 및 시행
8. 개인정보 보호 관련 자료의 관리
9. 처리 목적이 달성, 보유기간이 지난 개인정보의 파기

참고

공공

국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙 행정기관	➤	고위공무원단에 속하는 공무원
정무직공무원을 장 (長)으로 하는 국가기관	➤	3급 이상 공무원
고위공무원, 3급 공무원을 장으로 하는 국가기관	➤	4급 이상 공무원
기타 국가기관(소속 기관 포함)	➤	개인정보 처리 업무 부서장
시 · 도 및 시 · 도 교육청	➤	3급 이상 공무원
각급 학교	➤	행정사무 총괄자
기타 공공기관	➤	개인정보 처리 업무 부서장

민간

사업주(대표자) 또는 임원 (임원이 없는 경우, 개인정보 처리 업무 담당부서장)

- 개인정보 보호와 관련하여 이 법 및 다른 법령의 위반 사실을 알게 된 경우,
즉시 개선조치 시행, 필요 시 소속 기관의 장에게 보고
- 개인정보처리자는 보호책임자가 업무를 수행함에 있어서 정당한 이유 없이 불이익을 줘서는 안됨

개인정보 보호책임자 지정 (참고 이미지)

주식회사 ○○○

보존년한	1, 3, 5, 10년, 영구	인사발령				회 장
기안일자						(품 의) / 보 고
기안부서	홍보마케팅팀	결 재	담 당 자	팀 장	이 사	사 장
기 안 자	○○○					
최종결정	기, 부, 보류		인			
지시사항 및 합의의견						
제 목	개인정보 보호 책임자 변경의 건					

인사결정권자의
결재를 득하여 지정

상기 건을 다음과 같이 진행하고자 합니다.

- 사 유
- 조직개편 및 인사이동에 따른 개인정보 보호 책임자 변경

2. 변경일자 :

3. 개인정보 보호 책임자 변경

변 경(전)	변 경(후)
기획팀 ○○○ 팀장	홍보마케팅 ○○○ 팀장

※ 당사 사내 개인정보 보호업무 규정에 근거
- 주요 업무 및 인수인계 사항 개인정보 보호업무 규정 참고

- 기 타
- 품의 득 후 당사 홈페이지 내 "개인정보처리방침" 책임자 명 변경. 끝.

고시 변경 배경

- ▶ 접속기록 6개월 보관이 되레 관리부실 초래(18.8.21, 한겨레신문)
※ 2012년 총선 당시 서울 서대문구 13만명의 개인정보 불법 활용 정황
- ▶ 접속기록 관리부실로 무단열람 발생('12~'16 간 1만7천명 소명, 2,213건 징계('17 복지부 국감자료))
- ▶ 개인정보 유출사고 발생 1~2년 후 추적(한국은 사이버침해사고 발생 이후 발견시간은 2년 9개월, 2108, FireEye)
- ▶ 정보통신망법(기간통신사업자 2년), 신용정보보호법(감독규정 1년이상)

주요 내용

- ▶ 제2조(정의) 접속기록의 범위 확대 : 계정, 접속일시, **접속지 정보**, 접속자 정보, 수행업무
※ 접속한 자의 PC, 모바일기기 등 단말기 정보 또는 서버의 IP주소 등 접속 주소
- ▶ 제4조(내부관리계획의 수립 시행)
※ 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등
▶ 내부 관리계획의 이행 실태를 연 1회 이상으로 점검·관리 하여야 한다.
- ▶ 제8조 (접속기록의 보관 및 점검) 접속기록은 1년이상 보관, 월 1회 이상 점검
- ▶ 5만명 이상 고유식별정보 또는 민감정보를 처리하는 경우 2년 이상 보관



주요 내용

- ▶ 제4조(내부 관리계획의 수립·시행) 제1항 제7호의 “접속기록 보관 및 점검에 관한 사항”에 개인정보처리자의 업무 현황을 고려하여 다운로드 한 사유를 확인하여야 하는 다운로드 기준 마련 필요

■■■ 다운로드 사유확인이 필요한 기준 책정 예시 ■■■

- . (다운로드 정보주체의 수) 통상적으로 개인정보 처리 건수가 일평균 20건 미만인 소규모 기업에서 개인정보취급자가 100명 이상의 정보주체에 대한 개인정보를 다운로드 한 경우 사유 확인
- . (일정기간 내 다운로드 횟수) 개인정보취급자가 1시간 내 다운로드한 횟수가 20건 이상일 경우 단시간에 수차례에 걸쳐 개인정보를 다운로드 한 행위에 대한 사유 확인
- . (업무시간 외 다운로드 수행) 새벽시간, 휴무일 등 업무시간 외 개인정보를 다운로드 한 경우 사유 확인

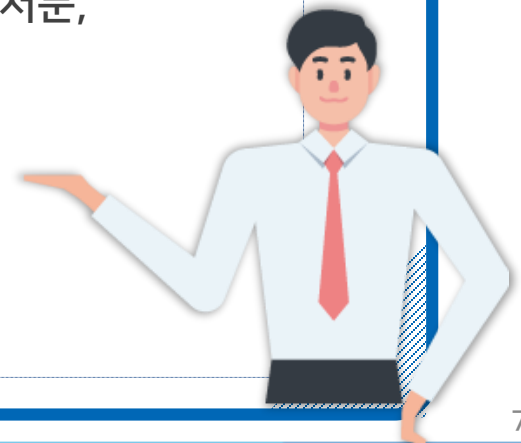


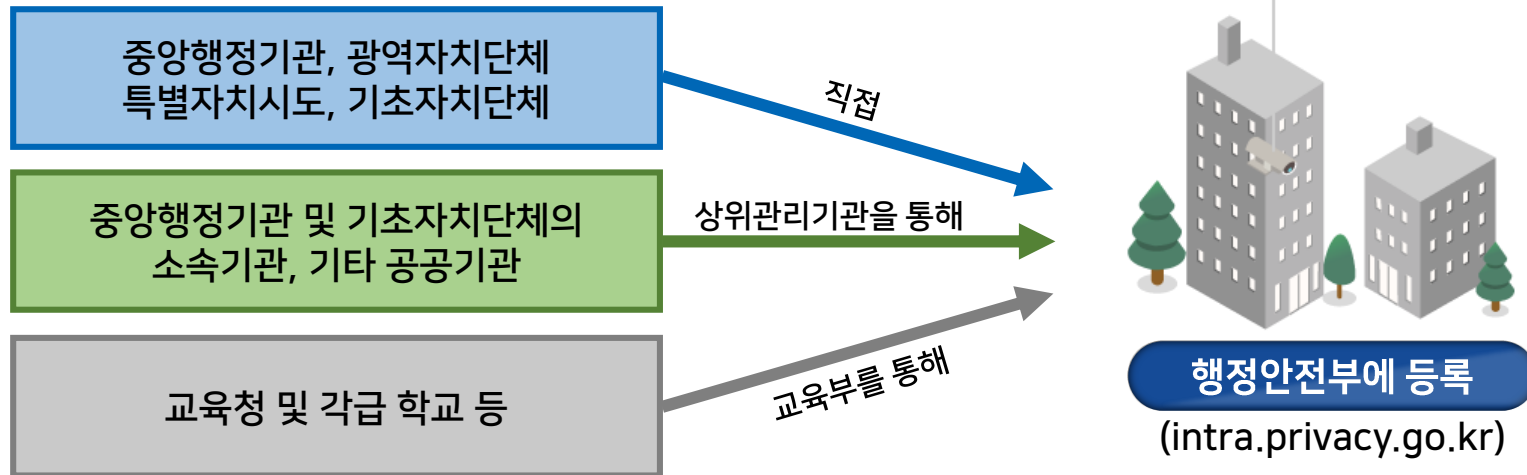
행정안전부장관에게 등록해야 하는 사항

- 개인정보파일의 명칭, 운영 근거 및 목적, 개인정보 항목
- 개인정보의 처리방법 및 보유기간, 반복적인 제공의 경우 제공받는 자
- 공공기관의 명칭, 개인정보의 정보주체 수, 개인정보 처리 업무 담당 부서
- 개인정보의 열람 요구를 접수·처리하는 부서와 열람을 제한·거절할 수 있는 개인정보의 범위 및 사유

등록 예외

- 국가 안전, 외교상 비밀 등 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
- 범죄의 수사, 공소의 제기 및 유지, 형 및 감호 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항
- 조세범처벌법, 관세법에 따른 범칙행위 조사에 관한 사항
- 내부적 업무처리만을 위하여 사용되는 개인정보파일
- 다른 법령에 따라 비밀로 분류된 개인정보파일





- ▶ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관에 등록. 변경 사항의 검토 및 적정성 판단을 요청한 후, 상위 관리기관의 확인을 받아 행정안전부에 등록하여야 함
- ▶ 교육청 및 각급 학교 등의 개인정보 보호책임자는 교육부에 등록. 변경 사항의 검토 및 적정성 판단을 요청한 후, 교육부의 확인을 받아 행정안전부에 등록하여야 함

개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 법에 부합하는지 등에 관하여 인증

정보보호 및 개인정보 보호 관리체계(ISMS-P)

☑ 인증의 기대 효과

- 체계적·지속적인 개인정보 보호 활동 가능
- 개인정보 침해 사고에 효율적 대응 가능
- 경영진 차원에서 상시 모니터링 체계 구축
- 개인정보 보호에 대한 국민·고객의 신뢰 향상

☑ 인증기관 : 한국인터넷진흥원

☑ 인증 유효기관 : 3년

☑ 신청기관 유형 : 공공기관, 대기업, 중소기업, 소상공인

* 정보통신서비스 제공자는 대기업 유형으로 인증

☑ 인증심사 기준 : 3개 영역 102개 인증기준

※ 인증기준 방법·절차 등은 고시 참조

☑ 정보보호 및 개인정보 보호 관리체계 인증에 관한 고시 시행 : 2018년 11월 7일

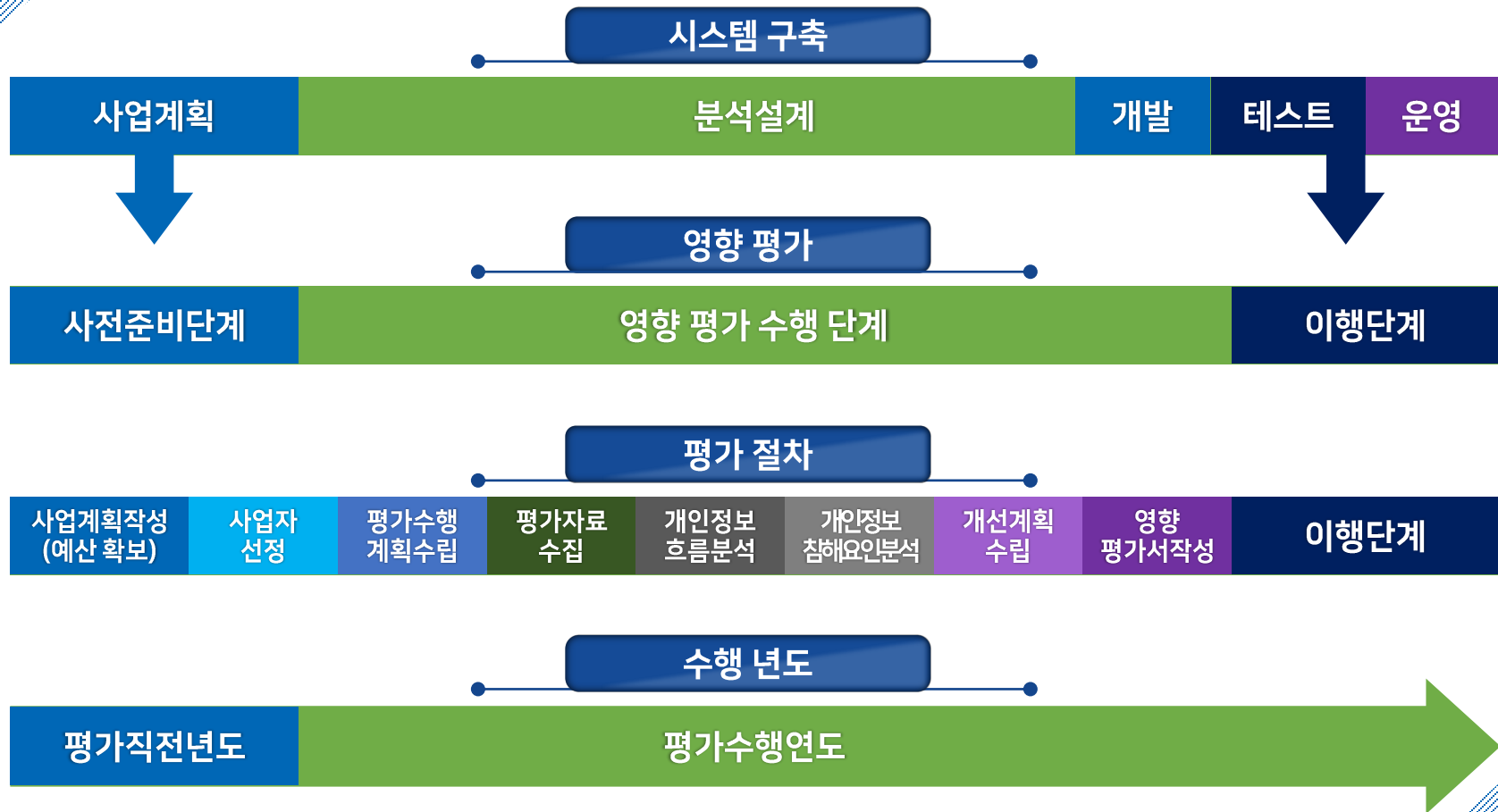


영역	분야	적용여부	
		ISMS	ISMS-P
1. 관리체계 수립 및 운영 (16개)	1. 1. 관리체계 기반 마련	○	○
	1. 2. 위험 관리	○	○
	1. 3. 관리체계의 운영	○	○
	1. 4. 관리체계의 점검 및 개선	○	○
2. 보호대책 요구사항 (64개)	2. 1. 정책, 조직, 자산 관리	○	○
	2. 2. 인적 보안	○	○
	2. 3. 외부자 보안	○	○
	2. 4. 물리 보안	○	○
	2. 5. 인증 및 권한관리	○	○
	2. 6. 접근통제	○	○
	2. 7. 암호화 적용	○	○
	2. 8. 정보시스템 도입 및 개발 보안	○	○
	2. 9. 시스템 및 서비스 운영관리	○	○
	2. 10. 시스템 및 서비스 보안관리	○	○
	2. 11. 사고 예방 및 대응	○	○
	2. 12. 재해복구	○	○
3. 개인정보 처리 단계별 요구사항 (22개)	3. 1. 개인정보 수집 시 보호조치	-	○
	3. 2. 개인정보 보유 및 이용 시 보호조치	-	○
	3. 3. 개인정보 제공 시 보호조치	-	○
	3. 4. 개인정보 파기 시 보호조치	-	○
	3. 5. 정보주체 권리보호	-	○

영향평가 수행대상

- ▶ 구축·운용 또는 변경하려는 개인정보파일로서 **5만명 이상의 정보주체**에 관한 **민감정보 또는 고유식별정보**의 처리가 수반되는 개인정보파일
- ▶ 구축·운용하고 있는 개인정보파일을 해동 공공기관 내부 또는 외부에서 구축 운용하고 있는 다른 개인정보파일과 **연계하려는 경우**로서 연계 결과 **50만명 이상의 정보주체**에 관한 개인정보가 포함되는 개인정보파일
- ▶ 구축·운용 또는 변경하려는 개인정보 파일로서 **100만명 이상의 정보주체**에 관한 개인정보파일





**정보시스템 구축 · 변경시
BPR/ISP(또는 분석 · 설계) 단계에서 영향평가를 수행**

개인정보 유출 통지 (제34조)



통지 방법

신고방법

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



**개인정보 유출 사실을 인지 하였을 경우에는 지체없이
정보주체에게 관련 사실 통지 및 전문기관에 신고 등 조치를 취해야 함**

개인정보 유출 신고 (제34조)



통지방법

신고 방법



신고대상	▶ 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우
신고기관	▶ 행정안전부, 전문기관(한국인터넷진흥원)
신고시기	▶ 5일 이내
신고방법	▶ 전화, 전화우편, 팩스
신고내용	▶ 통지내용, 유출피해 최소화 대책 및 조치 결과

개인정보 유출 사실을 인지하였을 경우에는 지체없이 정보주체에게
관련 사실 통지 및 **전문기관에 신고** 등 조치를 취해야 함

VI. 정보주체의 권리 보장과 피해구제 등

(개인정보 보호법 제4장)



“ 정보주체는 자신의 개인정보에 대한 열람·정정·삭제 요구 가능 ”

- ▶ 개인정보의 항목 및 내용
- ▶ 제3자 제공 현황
- ▶ 수집 · 이용 목적
- ▶ 개인정보 처리에 동의한 사실 및 내용
- ▶ 보유기간

※ 개인정보처리자가 공공기관인 경우에 행정안전부장관을 통해 열람요구 가능

열람 요구 시 10일 이내에 정보주체가 해당 개인정보를 열람할 수 있도록 조치

- ① 개인정보의 수집 출처
- ② 개인정보의 처리 목적
- ③ 개인정보 처리의 정지를 요구 할 권리가 있다는 사실

열람요청 기간 내에 열람할 수 없는 정당한 사유가 있을 때는,
정보주체에게 그 사유를 알리고 열람 연기 (사유 소멸 시 지체 없이 열람)

정보주체의 열람, 정정·삭제, 처리정지 요구권의 행사 방법과 절차 간소화

- 서면, 전화, 전자우편, 인터넷 등 정보주체가 쉽게 활용할 수 있는 방법 제공
- 개인정보를 수집한 창구 또는 방법에 의해 개인정보의 열람을 요구할 수 있도록 할 것
(다만, 해당 창구의 지속적 운영이 곤란한 경우 등 정당한 사유가 있는 경우 예외)
- 대표 홈페이지에 열람 요구 방법과 절차를 공개

Q

자동차보험계약만료 후, 다른 보험회사로 자동차
보험계약을 갱신하여 이전 보험회사에 개인정보
삭제를 요청하였더니 불가하다고 합니다. 개인정보처리자가
정보주체의 개인정보 삭제요청을 거부할 수 있나요?



A

개인정보처리자는 정보주체로부터 삭제요구를 받으면, 10일 이내에 그 개인정보를 조사하여
정보주체의 요구에 따라 해당 개인정보의 삭제 등 필요한 조치를 한 후 그 결과를 '개인 정보 정정·삭제
결과통지서' (『개인정보보호법』시행규칙 별지 제9호 서식)로 해당 정보주체에게 알려야 합니다.
단, 다른 법령에 따라 보존하여야 하는 경우에는 가능합니다.
정보주체의 정정·삭제 요구에 따라 필요한 조치를 취하지 않은 개인정보처리자에 대해서는
「개인정보 보호법」 제75조 제2항 제11호에 의거, 3천만원 이하의 과태료가 부과될 수 있습니다.

개인정보침해 신고상담



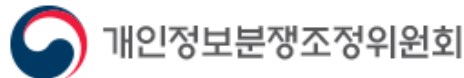
PRIVACY 개인정보침해 신고센터

행정안전부, 방송통신위원회, 한국인터넷진흥원이
국민의 개인정보보호를 위해 함께합니다.
정보통신강국의 미래를 개척하는 선봉이 되고자
다양한 업무를 수행하고 있습니다.

- 제도개선권고
- 행정처분 의뢰
- 수사 의뢰

관련근거
(개인정보 보호법 제62조)

개인정보분쟁조정



개인정보분쟁조정위원회

- 제도개선권고
- 손해배상 권고

관련근거
(개인정보 보호법 제40조)

민사소송



- 손해배상 청구

관련근거
(민법 제750조)

“ 징벌적 손해배상제도(제39조)와 법정 손해배상제도(제39조의2) ”

구 분	징벌적 손해배상제도	법정 손해배상제도
적용 요건	기업의 고의·중과실로 개인정보 유출 또는 동의 없이 활용하여 피해 발생	기업의 고의·과실로 개인정보가 분실·도난·유출된 경우
입증 책임	기업이 고의·중과실 없음을 입증 피해액은 피해자가 입증	기업이 고의·과실 없음을 입증 피해자에 대한 피해액 입증책임 면제
구제 범위	재산 및 정신적 피해 모두 포함	사실상 피해 입증이 어려운 정신적 피해
배상 규모	실제 피해액의 3배 이내 배상	300만원 이하의 범위에서 상당한 금액
적용 시기	2016년 7월 25일 이후 유출사고	

▶ 10년 이하 징역 또는 1억원 이하 벌금

- 공공기관의 개인정보처리업무를 방해할 목적으로 공공기관에서 처리하는 개인정보를 변경 또는 말소하여 공공기관의 업무수행에 심각한 지장을 초래한 자

▶ 5년 이하 징역 또는 5천만원 이하 벌금

- 정보주체의 동의 없이 개인정보를 제3자에게 제공한 자
- 민감정보 처리기준을 위반한 자
- 고유식별정보 처리기준을 위반한 자

▶ 3년 이하 징역 또는 3천만원 이하 벌금

- 영상정보처리기기 설치목적과 다른 목적으로 임의조작하거나 다른 곳을 비추는 자 또는 녹음 기능을 사용한 자
- 거짓 그 밖에 부정한 수단이나 방법에 의하여 개인정보를 취득하여 개인정보처리에 관한 동의를 얻은 행위를 한 자

▶ 2년 이하 징역 또는 2천만원 이하 벌금

- 안전성 확보에 필요한 보호조치를 취하지 아니하여 개인정보 분실·도난·유출·위조·변조·훼손당한 자

▶ 5천만원 이하 과태료

- 개인정보의 수집기준을 위반한 자
- 만 14세미만 아동의 개인정보 수집시 법정대리인 동의획득의무를 위반한 자
- 탈의실·목욕실 등 영상정보처리기기 설치 금지의무를 위반한 자

▶ 3천만원 이하 과태료

- 개인정보 수집·이용·제공 동의획득시, 목적 외 이용·제공 동의획득시, 직접 마케팅 업무위탁으로 인한 개인정보 제공시 정보주체에게 알려야할 사항을 알리지 아니한 자
- 정보주체 외로부터 수집한 개인정보를 고지하지 않은 자
- 개인정보를 파기하지 아니한 자
- 안전성 확보에 필요한 조치의무를 이행하지 아니한 자
- 영상정보처리기기 설치·운영기준 위반한 자
- 정보주체의 열람 요구를 부당하게 제한·거절한 자
- 정보주체의 정정요구에 따라 필요조치를 취하지 아니한자

▶ 1천만원 이하 과태료

- 미파기 개인정보의 별도 보존의무를 위반한 자
- 동의획득 방법을 위반하여 동의받은 자
- 영상정보처리기기 안내판 등 필요조치 이행하지 아니한 자
- 업무위탁시 공개의무를 위반한 자

참고

1.수집

2.이용

- 필요 최소한의 개인정보 수집
- 주민등록번호는 법령에 근거가 있는 경우 처리 가능
- 만14세미만 아동의 법정대리인 동의
- 동의 받을 때는 고지의무 사항 준수

3.제공

- 당초 수집 목적 외에 용도로 이용·제공 금지
- 개인정보 처리 업무위탁은 반드시 문서로 하고
- 수탁자에 대한 교육 및 감독 철저

4.관리 (보관)

- 개인정보 암호화하여 보관
- 접근권한, 접속기록 점검
- 내부관리계획 수립·이행 연 1회 이상 점검
- 개인정보파일 현황 정기적 파악 및 행정안전부 등록

5.파기

- 보유 목적 달성, 보유기간 경과 즉시 파기
- 복구·재생되지 않도록 철저히 파기



Privacy by Trust, Trust by Privacy!

질의문답

