

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례

믿을 수 있는 개인정보 활용, 신뢰사회의 기본입니다
Privacy by Trust, Trust by Privacy



Contents

- 1 개인정보 수집이용 동의서 검토
- 2 개인정보의 안전한 관리와 주요 조치사항
- 3 개인정보 보호법 법령 해석 사례
- 4 개인정보 관련 법령, 고시, 가이드라인 현황



1

개인정보 수집·이용 동의서 검토



개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



1. 개인정보 수집이용 동의서 검토

PIP교육진흥원 현황 주요 내용

▶ PIP 교육진흥원 주요 업무

기관 설립 목적

- 정보주체 및 개인정보처리자에게 개인정보의 중요성과 인식제고를 위한 전문 교육 서비스 제공
- 개인정보처리자를 위한 효과적인 보호 방안과 효율적인 개인정보 활용 방안 마련을 위한 전문화된 교육과정 제공
- 개인정보 보호 전문 자격제도 운영을 통한 전문가 양성

▶ PIP 교육진흥원 주요 업무

주요 업무 현황

- PIP교육센터 운영(회원제)
- 개인정보 보호 관련 온라인 교육과정 운영(일반과정, 전문가 과정)
- 개인정보 보호 전문가 자격시험(국가공인) 제도 운영
- 4개의 개인정보파일을 운영하고 있음

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



1. 개인정보 수집이용 동의서 검토

PIP교육진흥원 현황 주요 내용

▶ PIP 교육진흥원 개인정보파일 현황

| No | 개인정보 파일명 | 운영목적 |
|----|-----------------------------------|------------------------------|
| 1 | PIP교육센터 회원정보 | PIP교육센터 홈페이지 회원관리 |
| 2 | PIP교육센터 일반교육 및 전문교육 과정 수강생 정보 | PIP교육센터 일반교육 수료증 발급 및 수강생 관리 |
| 3 | 개인정보보호 전문가 자격 시험 응시자 및 자격증 보유자 정보 | PIP교육센터 전문교육 수료증 발급 및 수강생 관리 |
| 4 | PIP교육수강생 및 응시자민원대응 | 자격시험 응시자 및 자격증 보유자 관리 |

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



1. 개인정보 수집이용 동의서 검토

🔒 개인정보 수집이용 동의서 현황

▶ (실습내용) 다음은 정보주체가 PIP 교육진흥원 회원가입 웹 페이지 상 보여지는 개인정보 수집·이용 동의서의 전체 내용입니다. 배포된 PIP교육진흥원의 현황과 아래 동의서를 참고하여 잘못된 부분을 찾으시오.

✓ PIP교육진흥원은 회원관리와 개인정보보호 전문가 자격시험 합격자 관리를 위하여 다음과 같이 개인정보를 수집·이용하고자 합니다.

- 개인정보의 수집이용 목적: **회원가입 및 관리, 전문가 자격시험 합격자 관리**
- 개인정보 수집 항목: **회원ID, 패스워드, 이름, 주민등록번호, 휴대전화번호, 거주지 주소, 소속기관, 응시번호, 자격증 번호,**
- 개인정보의 보유기간: **회원탈퇴 후 즉시 파기**

※ 정보주체는 위의 개인정보 수집·이용에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 회원가입 및 개인정보보호 전문가 자격시험에 응시할 수 없습니다.

개인정보 수집·이용에 동의하십니까?

☐ 동의 | ☐ 미동의

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



1. 개인정보 수집이용 동의서 검토

🔒 개인정보 수집이용 동의서 현황

▶ (실습내용) 다음은 정보주체가 PIP 교육진흥원 회원가입 웹 페이지 상 보여지는 개인정보 수집·이용 동의서의 전체 내용입니다. 배포된 PIP교육진흥원의 현황과 아래 동의서를 참고하여 잘못된 부분을 찾으시오

✓ PIP교육진흥원은 회원관리와 개인정보보호 전문가 자격시험 합격자 관리를 위하여 다음과 같이 개인정보를 수집·이용하고자 합니다.

▪ 개인정보의 수집이용 목적: 회원가입 및 관리, 전문가 자격시험 합격자 관리

▪ 개인정보 수집 항목: 회원ID, 패스워드, 이름, 주민등록번호, 휴대전화번호, 거주지 주소, 소속기관, 응시번호, 자격증 번호

▪ 개인정보의 보유기간: 회원탈퇴 후 즉시 파기

※ 정보주체는 위의 개인정보 수집·이용에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 회원가입 및 개인정보보호 전문가 자격시험에 응시할 수 없습니다.

개인정보 수집·이용에 동의하십니까?

☒ 동의 | ☐ 미동의

- 회원가입 시에는 회원가입과 관련된 최소한의 사항만을 작성하여야 함
- 필요 최소한의 개인정보만 수집, 과도한 정보를 수집하고 있음
- 주민등록번호 수집 이용 근거가 고지되어 있지 않음
- 자격증 보유자에 대한 정보는 법령 상 준영구로 규정되어 있으나 기관 임의대로 파기하고 있음
- 주요정보 알기쉽게 표기(굵은 글씨, 색깔 등)
- 자격시험 합격자에 대한 개인정보 제3자 제공에 대한 고지와 동의가 이뤄지지 않음
- 개인정보 보호법 제15조제1항 제4호에 근거하여 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위한 경우 동의 없이 수집 가능
- 단, 입증책임은 개인정보처리자에게 있음

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



1. 개인정보 수집이용 동의서 검토

개인정보 수집이용 동의서 현황

- ▶ (실습내용) PIP 교육진흥원 회원가입 시 개인정보 수집·이용 동의서와 국가기술자격 시험 합격자에 대한 개인정보 수집·이용 동의서를 각각 올바르게 작성하시오.

앞에서 찾은 문제점을 개선하도록 동의서를 수정해 보세요

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



1. 개인정보 수집이용 동의서 검토

🔒 올바른 개인정보 수집이용 동의서 예시

▶ 회원가입 및 관리에 따른 개인정보 수집이용 동의서 예시

✓ (필수 수집) PIP교육진흥원은 회원가입과 회원관리를 위하여 다음과 같이 개인정보를 수집·이용하고자 합니다

- 개인정보의 수집이용 목적: **회원가입 처리 및 회원관리 업무, 민원응대**
- 개인정보 수집 항목: **회원ID, 비밀번호, 이름, 생년월일, 휴대전화번호, 이메일 주소**
- 개인정보의 보유기간: **회원탈퇴 시 파기**

※ 개인정보 수집·이용 근거법령 : 개인정보 보호법 제15조제1항제4호에 근거하여 정보주체와 체결한 계약의 이행을 위해 필요한 경우

✓ (선택 동의) PIP교육진흥원은 회원의 개인정보를 아래와 같이 수집 및 이용하고자 합니다.

- 개인정보의 수집이용 목적: **신청자에 한해 교육과정, 자격시험 일정 등 PIP교육진흥원 서비스에 대한 정보를 이메일로 제공**
- 개인정보 수집 항목: **이메일 주소**
- 개인정보의 보유기간: **회원탈퇴 시 파기**

※ 이용자는 위의 개인정보 수집·이용에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 이메일 수신에 불가능합니다.

개인정보 수집·이용에 동의하십니까?

☐ 동의 | ☐ 미동의

✓ PIP교육진흥원은 신청자에 한 해 교육과정, 자격시험 일정 등 PIP교육진흥원 서비스에 대한 정보를 이메일로 제공하고 있습니다. 해당 안내메일 수신에 동의하십니까?

정보수신에 동의하십니까?

☐ 동의 | ☐ 미동의

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



1. 개인정보 수집이용 동의서 검토

올바른 개인정보 수집이용 동의서 예시

▶ 국가기술자격증 보유자에 대한 개인정보 수집이용 동의서 예시

✓ PIP교육진흥원은 개인정보보호 전문가 자격시험 합격자 관리를 위하여 다음과 같이 개인정보를 수집·이용하고자 합니다.

- 개인정보의 수집이용 목적: 국가기술자격시험 합격자 관리
- 개인정보 수집 항목: 이름, 주민등록번호, 휴대전화번호, 이메일주소, 거주지 주소, 소속기관, 자격취득현황, 최종학력, 응시번호, 자격시험 평가점수, 사진
- 개인정보의 보유기간: 응시시험 경과 후 5년 후 파기

※ PIP교육진흥원 국가기술자격법 시행령 제26조(국가기술자격증의 관리 등) 4항 1호와 제33조의2(고유식별정보의 처리)에 따라 응시자의 응시자격여부를 확인하기 위하여 주민등록번호를 수집 및 이용합니다.

※ 개인정보 수집·이용 근거법령: 개인정보 보호법 제15조제1항제4호에 근거하여 정보주체와 체결한 계약의 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위해 필요한 경우

✓ PIP교육진흥원은 국가기술자격자 관리를 위하여 다음과 같이 개인정보를 제3자 제공하고자 합니다.

- 개인정보의 제공 목적: 국가기술자격자관리
- 개인정보 제공 항목: 이름, 주민등록번호, 시험 응시 상태, 합격여부, 전화번호, 이메일, 최종학력, 자격취득상태
- 제공받는 기관: 행정안전부, 한국고용정보원, 산업인력관리공단
- 보유기간: 준영구

※ 개인정보 제3자 제공은 법령에 근거한 사항으로 제3자 제공 미동의 시에는 국가기술자격자로 관리되지 않습니다.

※ 제3자 제공 근거법령: 자격기본법 제10조(자격정보시스템의 구축 등), 국가기술자격법 제7조(국가기술자격 정보체계의 구축), 국가기술자격법 시행령 제8조(국가기술자격 정보체계의 구축 및 운영)

개인정보 제3자 제공에 동의하십니까?

☐ 동의 | ☐ 미동의

2

개인정보의 안전한 관리 주요 조치사항



개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



2. 개인정보의 안전한 관리

🔒 개인정보처리시스템의 범위(용어정의)

▶ 개인정보처리자

- "개인정보처리자"란 업무를 목적으로 개인정보파일을 운영하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말함

▶ 개인정보책임자

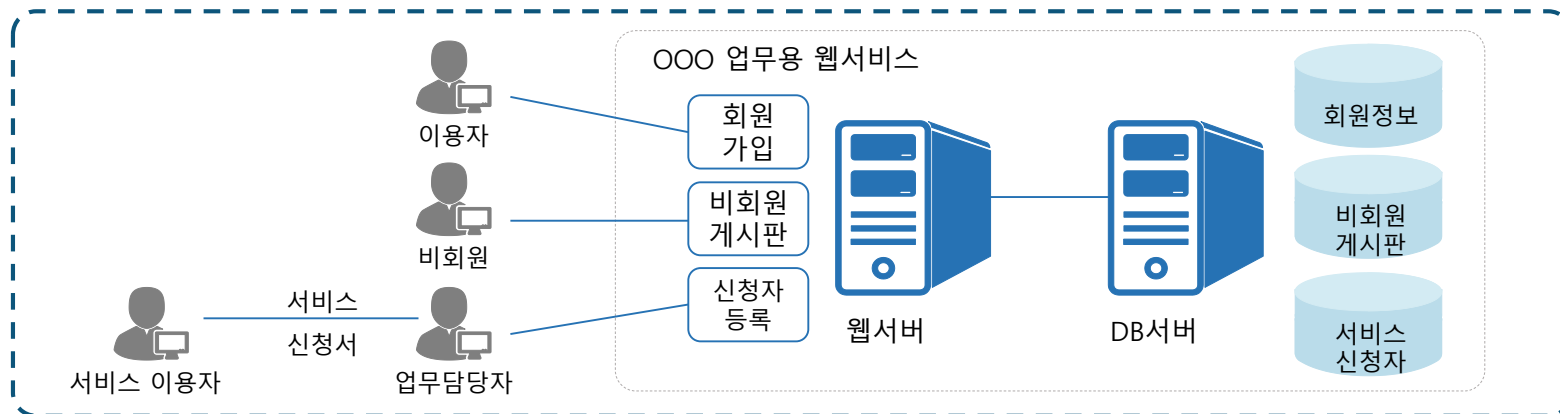
- 개인정보처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자

▶ 개인정보취급자

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

▶ 개인정보처리시스템

- 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템



개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



2. 개인정보의 안전한 관리

🔒 안전조치의무(제29조) / 시행령제30조(개인정보의 안전성 확보 조치)

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

- 1 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행·점검
- 2 개인정보에 대한 접근 권한을 제한하기 위한 조치
- 3 개인정보에 대한 접근을 통제하기 위한 조치
- 4 개인정보를 안전하게 저장·전송하는데 필요한 조치
- 5 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
- 6 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대해 컴퓨터바이러스, 스파이웨어, 랜섬웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하는 등의 기능이 포함된 프로그램의 설치·운영과 주기적 갱신·점검 조치
- 7 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

위반 시 3천만원 이하의 과태료



2. 개인정보의 안전한 관리

🔒 안전성 확보조치를 취할 의무 위반의 판단(판례)

✓ 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률 상 또는 계약상 의무를 위반하였는지 여부는 다음의 사항을 종합적으로 고려 필요
[대법원 2018. 12. 28, 선고, 2017다207994, 판결]

- 해킹 등 침해사고 당시 일반적으로 알려져 있는 정보보안 기술 수준
- 정보통신서비스 제공자의 업종과 영업 규모
- 정보통신서비스 제공자가 취하고 있던 전체적인 보안조치의 내용
- 정보보안조치에 필요한 경제적 비용 및 그 효용의 정도
- 해킹기술 수준과 정보보안기술 발전 정도에 따른 피해 발생 회피 가능성
- 정보통신서비스제공자가 수집한 개인정보의 내용과 개인정보 누출로 인하여 이용자가 입게 되는 피해 정도 등

✓ 개인정보의 기술적·관리적 보호조치 기준(정보통신부 고시 제2005-18호 및 제2007-3호, 이하 '이 사건 고시'라 한다)은 해킹 등 침해사고 당시의 기술수준 등을 고려하여 정보통신서비스제공자가 구 정보통신망법 제28조 제1항에 따라 준수해야 할 기술적·관리적 보호조치를 구체적으로 규정하고 있으므로, 정보통신서비스제공자가 이 사건 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였다면, 특별한 사정이 없는 한, 정보통신서비스제공자가 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였다고 보기는 어렵다
[대법원 2015. 2. 12, 선고, 2013다 43994, 2013다44003(병합) 판결]

※ 안전성 확보조치의 판례에 대한 분석은 고급과정에서 교육 진행 중

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



2. 개인정보의 안전한 관리

안전조치의무(제29조)

▶ 개인정보의 안전성 확보조치 기준과 기술적 관리적 보호조치 기준 통합

| (종전) 확보조치 기준 | (종전) 보호조치 기준 | 개정 고시 | 유예 기간 |
|---------------------|-------------------------|---------------------|--|
| | | 제1장 총칙 | <div> 유예기간 ('24.9.15.부터 시행) [특례대상] : 종전의 「개인정보의 기술적·관리적 보호조치 기준」 적용대상인 개인정보처리자 [일반대상] : 종전의 「개인정보의 안전성 확보조치 기준」 적용대상인 개인정보처리자 </div> |
| 제1조(목적) | 제1조(목적) | 제1조(목적) | |
| 제2조(정의) | 제2조(정의) | 제2조(정의) | |
| | | 제2장 개인정보의 안전성 확보조치 | |
| 제3조(안전조치 기준 적용) | | 제3조(안전조치 기준 적용) | |
| 제4조(내부 관리계획의 수립·시행) | 제3조(내부 관리계획의 수립·시행) | 제4조(내부 관리계획의 수립·시행) | |
| 제5조(접근 권한의 권리) | 제4조(접근 통제) ①, ②, ③, ⑦ ⑧ | 제5조(접근 권한의 권리) | [특례대상] 제5조제6항 [일반대상] 제5조제6항 중 정보주체에 관한 개정규정 |
| 제6조(접근통제) | 제4조(접근통제) ④, ⑤, ⑥, ⑨, ⑩ | 제6조(접근통제) | |
| 제7조(개인정보의 암호화) | 제6조(개인정보의 암호화) | 제7조(개인정보의 암호화) | [일반대상] 제7조제4항, [특례대상] 제7조제6항 |
| 제8조(접속기록의 보관 및 점검) | 제5조(접속기록의 위·변조 방지) | 제8조(접속기록의 보관 및 점검) | [특례대상] 제8조 제2항 |
| 제9조(악성프로그램 등 방지) | 제7조(악성프로그램 등 방지) | 제9조(악성프로그램 등 방지) | |
| 제10조(관리용 단말기의 안전조치) | | | |

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



2. 개인정보의 안전한 관리

안전조치의무(제29조)

▶ 개인정보의 안전성 확보조치 기준과 기술적 관리적 보호조치 기준 통합

| (종전) 확보조치 기준 | (종전) 보호조치 기준 | 개정 고시 | 유예 기간 |
|---|------------------------|------------------------------------|----------------------|
| 제11조(물리적 안전조치) | 제8조(물리적 접근 방지) | 제10조(물리적 안전조치) | |
| 제12조(재해·재난 대비 안전조치) | | 제11조(재해·재난 대비 안전조치) | [특례대상] 제11조 |
| | 제9조(출력·복사 시 보호조치) | 제12조(출력·복사 시 보호조치) | [일반대상] 제12조 제2항 |
| | 제10조(개인정보 표시 제한 보호 조치) | | |
| 제13조(개인정보의 파기) | | 제13조(개인정보의 파기) | |
| ※ 공공부문 개인정보 유출방지 대책 반영 (시행령 제30조의2제1항) | | 제3장 공공시스템 운영기관 등의 개인정보 안전성 확보조치 | 공공시스템운영기관과 공공시스템이용기관 |
| | | 제14조(공공시스템운영기관의 안전 조치 기준 적용) | |
| | | 제15조(공공시스템운영기관의 내부 관리계획의 수립·시행) | |
| | | 제16조(공공시스템운영기관의 접근 권한의 관리) | |
| | | 제17조(공공시스템운영기관의 접속 기록의 보관 및 점검) | |



2. 개인정보의 안전한 관리

안전조치의무 주요 조치사항 및 방법

▶ 내부관리계획의 수립·시행 및 점검 (제4조)

- 1 개인정보처리자가 내부 관리계획의 수립 및 시행, 이행 점검 하도록 개정
- 2 적용대상: 개인정보처리자 (단, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우 생략 가능)
- 3 내부 관리계획의 수립 및 시행 관련 사항
 - ✓ 개인정보책임자 및 개인정보취급자를 대상으로 차등화하여 정기적 교육 실시
※고려사항: 사업규모, 개인정보 보유 수, 업무성격 등
 - ✓ 내부 관리계획에 중요한 변경 사항이 있는 경우 즉시 반영, 수정, 시행, 수정 이력 관리
- 4 내부 관리계획의 이행 실태 점검·관리 관련 사항
 - ✓ 역할: 개인정보 보호책임자 ✓ 기간: 연 1회 이상
 - ✓ 결과보고: 내부 관리계획의 이행 실태 (접근권한 관리, 접속기록 보관 및 점검, 암호화 등) 점검 결과



2. 개인정보의 안전한 관리

안전조치의무 주요 조치사항 및 방법

▶ 내부관리계획의 수립·시행 및 점검 (제4조)

(중전) 확보조치 기준

제4조(내부 관리계획의 수립·시행)

- ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다.

(중전) 보호조치 기준

제4조(내부 관리계획의 수립·시행)

- ① 정보통신서비스 제공자 등은 다음 각 호의 사항을 정하여 개인정보보호 조직을 구성·운영하여야 한다.
- ② 정보통신서비스 제공자 등은 제1항 및 제2항에 대한 세부 계획, 제4조부터 제8조까지의 보호조치 이행을 위한 세부적인 추진방안을 포함한 내부관리계획을 수립·시행하여야 한다.

개정고시

제4조(내부 관리계획의 수립·시행 및 점검)

- ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다.

다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다.

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



2. 개인정보의 안전한 관리

🔒 안전조치의무 주요 조치사항 및 방법

▶ 내부관리계획의 수립·시행 및 점검 (제4조)

- ✓ 종전 일반규정과 특례규정의 유사한 내용을 통합
- ✓ 4호. 개인정보취급자에 대한 관리·감독에 관한 사항 추가
- ✓ 10호. 개인정보를 처리하는 개인정보처리자는 개인정보가 유출·변조·훼손되지 않도록 개인정보를 처리하는 환경, 기기, 설비 등에 대하여 취약점을 점검
- ✓ 15호. 개인정보 처리 방법 및 환경 등의 변화로 인하여 내부 관리계획에 중요한 변경이 있을 때에는 변경 사항 즉시 반영

내부 관리계획의 포함 사항

- 01 개인정보 보호 조직의 구성 및 운영에 관한 사항
- 02 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
- 03 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
- 04 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항
- 05 접근 권한의 관리에 관한 사항
- 06 접근 통제에 관한 사항
- 07 개인정보의 암호화 조치에 관한 사항
- 08 접속기록 보관 및 점검에 관한 사항
- 09 악성프로그램 등 방지에 관한 사항
- 10 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항
- 11 물리적 안전조치에 관한 사항
- 12 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
- 13 위험 분석 및 관리에 관한 사항
- 14 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
- 15 개인정보 내부 관리계획의 수립, 변경 및 승인에 관한 사항
- 16 그 밖에 개인정보 보호를 위하여 필요한 사항



2. 개인정보의 안전한 관리

안전조치의무 주요 조치사항 및 방법

▶ 접근권한 관리

1 최소 범위로 권한 차등부여 및 변경·말소

- ✓ 업무별 접근 가능한 메뉴 및 상세권한 세분화 및 최소한의 차등 부여
- ✓ 업무 변경시 지체없이 권한 변경 및 말소필요

2 접근권한 부여, 변경, 말소 내역 3년 이상 보관

- ✓ 접근권한 부여·변경·말소 내역 3년간 보관
- ✓ 권한변경 내역의 누적 기록·관리
- ✓ 접근권한에 관한 기록 : ① 계정신청정보(ID, 사용자), ② 신청일시, ③ 권한 상태 (권한 및 생성/변경/말소, ④ 승인자 및 발급자 정보, ⑤ 신청 및 발급 사유



2. 개인정보의 안전한 관리

안전조치의무 주요 조치사항 및 방법

▶ 접근권한 관리

3 1인 1계정 발급 및 공유 금지

- ✓ **정당한 사유가 없는 한 개인정보취급자 별로 계정 발급 및 다른 취급자와 공유 금지**
 - ※ 정당한 사유 : root 등 시스템에서 고정된 계정 1개만 생성이 가능한 경우로서 다른 계정 생성이 기술적으로 불가능한 경우 등

5 권한 도용 방지

- ✓ **개인정보취급자 또는 정보주체가 일정 횟수 이상 인증 실패 시 접근 제한**
 - ※ 정보통신서비스제공자의 경우 1년간 유예
 - ※ 정보주체에게 확대되는 규정은 일반 개인정보처리자도 1년간 유예

4 인증수단 안전하게 관리

- ✓ **개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리**
- ✓ **비밀번호 외 생체인증 등 다양한 인증수단 활용**
- ✓ **비밀번호를 인증수단으로 이용하는 경우 스스로의 환경에 맞는 비밀번호 작성 규칙을 자율적으로 적용**



2. 개인정보의 안전한 관리

안전조치의무 주요 조치사항 및 방법

▶ 접근통제

1 불법적인 접근 및 침해사고 방지를 위한 안전조치

- ✓ 개인정보처리시스템의 IP 주소 등을 제한하여 비인가자의 접근 제한
- ✓ IP 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응

2 외부 접근 통제

- ✓ 원칙적인 외부 접근 차단
- ✓ 불가피한 외부 접속 시 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단 적용
- ✓ 이용자 외 개인정보처리시: 가상사설망 등 안전한 접속수단 또는 안전한 인증 수단 적용 가능

3 노출 및 공유 설정 제한

- ✓ 인터넷 홈페이지, P2P, 공유 설정 등을 통하여 권한 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 조치

4 세션 타임 아웃

- ✓ 일정시간 이상 업무처리를 하지 않는 경우에는 자동 접속 차단 등 필요한 조치

5 모바일 기기 관리

- ✓ 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치



2. 개인정보의 안전한 관리

🔒 안전조치의무 주요 조치사항 및 방법

▶ 접근통제

6 망 분리

✓ 적용 대상

- 전년도 말 기준 직전 3개월간 그 개인정보가 저장관리되고 있는 이용자 수가 일일평균 100만명 이상인 개인정보처리자

※ **이용자**: 정보통신망법에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자

※ 이용자의 법적 정의에 따라 **망분리**는 정보통신서비스제공자에게만 적용

✓ 조치 사항

- 개인정보처리시스템에서 개인정보를 ① 다운로드 또는 ② 파기할 수 있거나 개인정보처리시스템에 대한 ③ 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등에 대한 인터넷망 차단 조치 필요

※ 다운로드: 개인정보처리시스템에 직접 접속하여 취급자의 컴퓨터 등에
개인정보를 엑셀, 워드, 텍스트, 이미지 등 파일 형태로 저장 하는 것을 의미

※ 파기: 개인정보처리시스템에 저장된 개인정보파일, 레코드, 테이블 또는 데이터베이스(DB)를 삭제하는 것을 의미

※ 접근권한설정: 개인정보처리시스템에 접근하는 개인정보취급자에게 다운로드, 파기 등의 접근권한을 설정하는 것을 의미함



2. 개인정보의 안전한 관리

안전조치의무 주요 조치사항 및 방법

▶ 접근통제

6 망 분리

- ✓ 다만, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제2조제3호*에 따른 클라우드 컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성운영하는 경우에는 해당 서비스에 대한 접속 외에는 인터넷을 차단하는 조치를 하여야 함
 - ※ 제2조제3호 “클라우드컴퓨팅서비스”란 클라우드컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신자원을 제공하는 서비스로서 대통령령으로 정하는 것을 말한다.
- ✓ 논리적 망 분리 및 물리적 망 분리 모두 가능



2. 개인정보의 안전한 관리

안전조치의무 주요 조치사항 및 방법

▶ 개인정보의 암호화

1 인증정보 암호화

- ✓ 비밀번호, 생체인식 정보 등 인증정보를 저장 또는 정보통신망을 통하여 송수신하는 경우
 - 안전한 알고리즘으로 암호화
 - 비밀번호는 복호화되지 않도록 일방향 암호화(SHA-256 등) 적용

2 이용자 개인정보 암호화

- ✓ 이용자의 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 생체인식정보는 안전한 알고리즘으로 암호화 하여 적용



2. 개인정보의 안전한 관리

🔒 안전조치의무 주요 조치사항 및 방법

▶ 개인정보의 암호화

3 고유식별정보 암호화

✓ 인터넷 구간/인터넷 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)에 고유식별정보 저장 시 암호화

✓ 내부망에 고유식별정보를 저장하는 경우

※ 다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 아래 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행 가능

- ① 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
- ② 암호화 미적용시 위험도 분석에 따른 결과

4 정보통신망을 통한 인터넷망 구간 송·수신 시

✓ 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송수신하는 경우 암호화



2. 개인정보의 안전한 관리

🔒 안전조치의무 주요 조치사항 및 방법

▶ 개인정보의 암호화

5 기기 및 저장 매체 저장 시

- ✓ 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조 저장매체 등에 저장 시 암호화한 후 저장

6 암호키 관리

- ✓ 적용 대상
 - 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관
 - 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체
- ✓ 조치사항
 - 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행
 - ※ 암호 키는 암호화된 데이터를 복호화 할 수 있는 정보이므로 암호 키의 안전한 사용과 관리는 매우 중요하며, 라이프사이클 단계별 암호 키 관리 절차를 수립·시행 필요

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



2. 개인정보의 안전한 관리

🔒 안전조치의무 주요 조치사항 및 방법

▶ 개인정보의 암호화

| 구분 | 정보통신망을 통한 송·수신시 | | 저장시 | | | | 개인정보취급자 컴퓨터, 모바일기 기, 보조매체 등에 저장시 | |
|-----------------------|--|--|---|---|---------------|--------------------------|---|------|
| | 정보통신망 | 인터넷망 | 저장위치 무관 | | 인터넷구간, DMZ | 내부망 | | |
| 이용자의 개인정보 | 인증정보 (비밀번호, 생체 인식정보 등) | 개인정보 *일반 개인 정보처리자 의 경우 2024.9.15 시행 | 인증정보 (비밀번호, 생 체인식정보) *단, 비밀번호 는 일방향 암 호화 | 신용카드 번호, 계좌번호, 생체인식정보 - | 주민등 록번호 | 여권번호, 운전면허번호, 외국인등록번호 | | 개인정보 |
| 이용자 외 정보주체 개인정보 | | | | | | 고유식별정보(주민 등록번호 제외) | *내부망 저장시 암호화하거나 영향평가 또는 위함도 분석을 통해 암호화 미 적용 가능 | |
| 암호키 관리 | 10만명 이상 대기업·중견기업·공공기관, 100만명 이상 중소기업·단체 : 암호키 생성, 이용, 보관,배포 및 파기 등에 관한 절차를 수립·시행 | | | | | | | |

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



2. 개인정보의 안전한 관리

🔒 안전조치의무 주요 조치사항 및 방법

▶ 접속기록 보관 및 관리

1 접속기록 1년 이상 보관

- ✓ 개인정보취급자가 접속한 사실을 알 수 있도록 전자적으로 자동 기록되도록 조치
- ✓ 필요 정보
 - ① 식별자 : 시스템에 접속한 자를 식별할 수 있도록 부여된 정보
 - ② 접속일시(연, 월, 일, 시, 분, 초) : 접속한 시점 또는 업무를 수행한 시점
 - ③ 접속지(IP 주소 등) : 접속한 취급자의 컴퓨터, 모바일기기 등 주소
 - ④ 정보주체 정보 : 개인정보 취급자가 누구의 개인정보를 처리했는지 알 수 있는 이름, ID 등
 - ⑤ 수행업무(조회, 저장, 수정, 삭제, 다운로드 등) : 취급자가 시스템에서 처리한 정보주체에 관한 수행업무 내용을 알 수 있는 정보
- ✓ 보유기간
 - 모든 개인정보처리시스템 : 최소 1년 이상
 - 유출 시 피해가능성이 높은 개인정보 (5만명 이상 개인정보, 고유식별정보 또는 민감정보) : 최소 2년 이상
 - 기간통신사업자 : 최소 2년 이상

2 접속기록 월 1회 이상 점검

- ✓ 최소 월 1회 이상 점검
- ✓ 비정상 행위 탐지 및 적절한 대응조치 적용
- ✓ 점검 대상
 - ① 점검주체 (개인정보보호 부서, 감사부서, 개인정보보호 전문업체 등)
 - ② 점검시기 : 최소 월 1회 이상
 - ③ 점검항목 및 내용 : 비인가된 개인정보 처리 및 대량의 개인정보 다운로드 등 비정상 행위, 접속기록의 위변조 여부 등
 - ④ 점검 후속조치 : 개선조치, 결과보고 등
- ✓ 접속기록이 위변조 및 도난, 분실되지 않도록 안전한 보관
(기존) 별도의 물리적인 저장 장치 보관, 정기적인 백업 -> (개정 개인정보 보호법) 안전하게 보관하기 위한 조치
(예시)
 - ① 접속기록의 상시 백업 : 별도의 보조저장매체, 저장장치 등에 보관
 - ② 저장 시 CD-ROM, DVD-R, WORM 등과 같은 덮어쓰기 방지 매체 사용
 - ③ 접속기록을 수정 가능한 매체(하드디스크 등)에 백업하는 경우 위변조 여부를 확인할 수 있는 정보를 별도의 장비에 보관

※ 안전성 확보조치와 관련된 보다 자세한 내용은 중급과정에서 교육 진행 중



2. 개인정보의 안전한 관리

🔒 개인정보 처리방침의 수립 및 공개(제30조)

▶ 개인정보 처리방침의 주요 내용

1. 개인정보의 **처리 목적**
2. 개인정보의 **처리 및 보유기간**
3. 개인정보의 **제3자 제공**에 관한 사항 (해당하는 경우에만)
4. 개인정보의 **파기절차 및 파기방법**(개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목)
5. 민감정보의 **공개 가능성 및 비공개**를 선택하는 방법(해당되는 경우에만)
6. 개인정보 처리의 **위탁**에 관한 사항(해당하는 경우에만)
7. **가명정보의 처리** 등에 관한 사항(해당되는 경우에만)
8. **정보주체와 법정대리인의 권리·의무 및 그 행사방법**에 관한 사항
9. **개인정보 보호책임자의 성명 또는 개인정보 보호업무** 및 관련 고충사항을 처리하는 **부서의 명칭과 전화번호 등 연락처**
10. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만)
11. 처리하는 개인정보의 **항목**
12. 개인정보의 **안전성 확보조치**에 관한 사항
13. 개인정보 처리방침 변경에 관한 사항

개인정보 처리방침은 **인터넷 홈페이지에 지속적으로 게재**하여 공개해야 함

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



2. 개인정보의 안전한 관리

🔒 개인정보 처리방침의 수립 및 공개(제30조)

▶ 개인정보 처리방침 기재사항

| 구분 | 기재사항 | 적용 |
|----|----------------------------------|----------|
| 1 | 제목 및 서문 | 의무 |
| 2 | 개인정보의 처리목적 | 의무 |
| 3 | 개인정보의 처리 및 보유기간 | 의무 |
| 4 | 처리하는 개인정보의 항목 | 의무 |
| 5 | 만 14세미만 아동의 개인정보 처리에 관한 사항 | 권장, 해당 시 |
| 6 | 개인정보의 제3자 제공에 관한 사항 | 의무, 해당 시 |
| 7 | 개인정보의 파기 절차 및 방법에 관한 사항 | 의무 |
| 8 | 미이용자의 개인정보 파기 등에 관한 조치 | 권장, 해당 시 |
| 9 | 민감정보의 공개 가능성 및 비공개를 선택하는 방법 | 의무, 해당 시 |
| 10 | 개인정보 처리업무의 위탁에 관한 사항 | 의무, 해당 시 |
| 11 | 개인정보의 국외 이전에 관한 사항 | 권장, 해당 시 |
| 12 | 가명정보의 처리 등에 관한 사항 | 의무, 해당 시 |
| 13 | 정보주체와 법정대리인의 권리 의무 및 행사방법에 관한 사항 | 의무 |

| 구분 | 기재사항 | 적용 |
|----|---|----------|
| 14 | 개인정보의 안전성 확보조치에 관한 사항 | 의무 |
| 15 | 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항 | 의무, 해당 시 |
| 16 | 행태정보의 수집 이용 제공 및 거부 등에 관한 사항* | 의무, 해당 시 |
| 17 | 추가적인 이용 제공 관련 판단 기준* | 의무, 해당 시 |
| 18 | 가명정보 처리에 관한 사항 | 의무, 해당 시 |
| 19 | 개인정보 보호 책임자에 관한 사항 | 의무 |
| 20 | 국내 대리인 지정에 관한 사항 | 의무, 해당 시 |
| 21 | 개인정보의 열람청구를 접수 처리하는 부서 | 의무 |
| 22 | 정보주체의 권익침해에 대한 구제방법 | 의무 |
| 23 | 고정형 및 이동형 영상정보처리기기 운영 관리에 관한 사항 | 권장, 해당 시 |
| 24 | 개인정보 처리방침의 변경에 관한 사항 | 의무 |
| 25 | 그밖에 개인정보처리자가 개인정보 처리 기준 및 보호조치 등에 관하여 자율적으로 개인정보 처리방침에 포함하여 정한 사항 | 권장, 해당 시 |



2. 개인정보의 안전한 관리

🔒 개인정보 처리방침의 수립 및 공개(제30조)

▶ 행태정보의 처리와 개인정보 처리방침 상 표기

✓ 개인정보처리자가 정보주체의 온라인 행태정보를 처리하고 이를 기반으로 '온라인 맞춤형 광고' 등을 제공하는 경우 그 수집·이용에 관한 사항 및 거부 등에 대해 기재

① 수집하는 행태정보의 항목, ② 수집방법, ③ 수집목적, ④ 보유이용기간 및 이후 정보처리 방법 ⑤ 제3자 제공 시 제공받는자 항목, 목적 등 ⑥ 동의를 거부할 수 있는 권리 및 방법 등의 기재

※ 단, 상품 및 서비스의 판매 홍보 목적이 아니며, 제공하는 서비스와 관련된 이용자 편의 제공을 위해 사용 환경(UX, UI 등)을 이용자별로 상이하게 구성하는 등의 맞춤형 서비스 제공은 온라인 맞춤형 광고에 해당하지 않음

✓ 작성 예시

- ① 개인정보처리자는 서비스 이용과정에서 정보주체에게 최적화된 맞춤형 서비스 및 혜택, 온라인 맞춤형 광고 등을 제공하기 위하여 행태정보를 수집 이용하고 있습니다.
- ② 개인정보 처리자는 다음과 같이 행태정보를 수집합니다.

| 수집하는 행태정보의 항목 | 행태정보 수집 방법 | 행태정보 수집목적 | 보유·이용기간 및 이후 정보처리 방법 |
|----------------------------------|-----------------------------|--|----------------------|
| 이용자의 웹사이트/앱 서비스 방문이력, 검색이력, 구매이력 | 이용자의 웹사이트 및 앱 방문/실행 시 자동 수집 | 이용자의 관심, 성향에 기반한 개인 맞춤형 상품추천 서비스(광고포함)를 제공 | 수집일부터 **일 후 파기 |



2. 개인정보의 안전한 관리

🔒 개인정보 처리방침의 수립 및 공개(제30조)

▶ 추가적인 이용제공의 판단과 개인정보처리방침 공개

- ✓ 개인정보처리자가 법 제15조제3항 또는 제17조제4항에 따라 정보주체의 동의없이 개인정보를 이용 또는 제공하려는 경우 영 제14조의 2에 따라 각 호의 사항을 고려해야 하며, 고려사항에 대한 판단기준을 법 제30조 제1항에 따른 개인정보 처리방침에 미리 공개해야 함

※ 추가적인 이용제공 시 고려사항에 대한 판단기준은 사업자/단체 스스로 **자율적으로 판단**하여 작성 공개하여야 함
※ 법 제31조제1항에 따른 개인정보 보호책임자가 해당 기준에 따라 개인정보의 추가적인 이용 또는 제공을 하고 있는지 여부를 점검해야 함

✓ 작성 예시

- ① 개인정보처리자는 법 제15조제3항 또는 제17조제4항에 따라 개인정보보호법 시행령 제14조의 2에 따른 사항을 고려하여 정보주체의 동의없이 개인정보를 추가적으로 이용 제공할 수 있습니다.

| 항목 | 이용 제공 목적 | 보유 및 이용기간 |
|------------|-------------------------------|---------------|
| 이름 연락처, 주소 | 정기적으로 제공하는 OO서비스 관련 추가 안내물 발송 | 목적 달성 후 즉시 파기 |

- ② 이에 따라 000은 정보주체의 동의 없이 추가적인 이용 제공을 하기 위해서 다음과 같은 사항을 고려하였습니다.

- ✓ 개인정보를 추가적으로 이용 제공하려는 목적이 당초 수집목적과 관련성이 있는지 여부
- ✓ 개인정보를 수집한 정황 또는 처리관행에 비추어 볼 때 추가적인 이용 제공에 대한 예측 가능성이 있는지 여부
- ✓ 개인정보의 추가적인 이용 제공이 정보주체의 이익을 부당하게 침해하는지 여부
- ✓ 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



2. 개인정보의 안전한 관리

🔒 개인정보 보호책임자의 지정 요건(제31조)

➤ 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

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



2. 개인정보의 안전한 관리

🔒 개인정보파일의 등록 및 공개(제32조) : 공공기관만 해당

▶ 개인정보파일을 운용하는 공공기관이 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

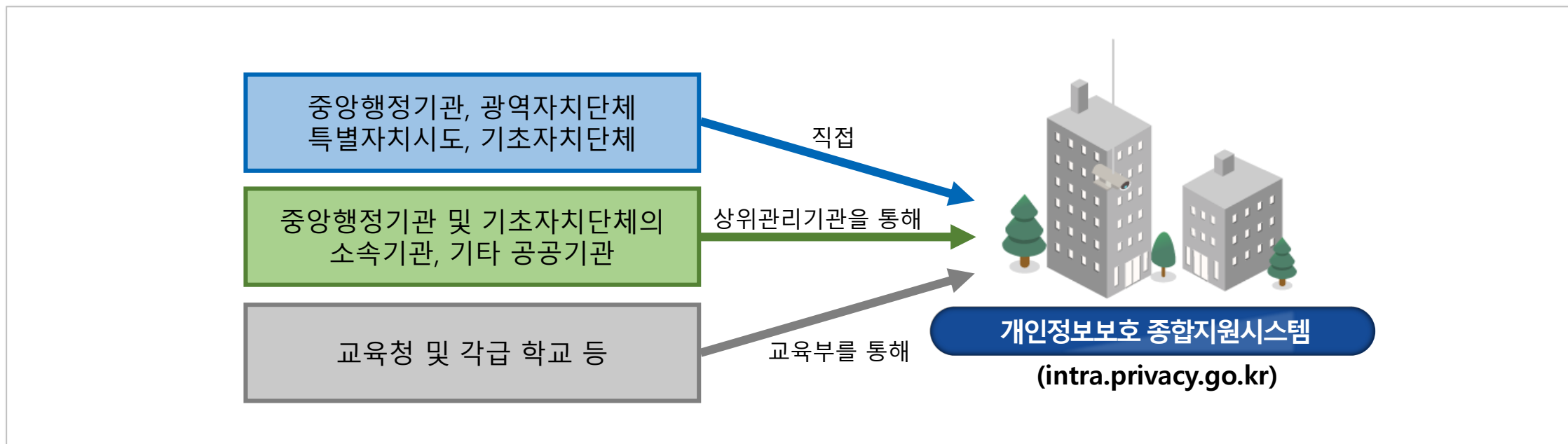


개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



2. 개인정보의 안전한 관리

🔒 개인정보파일의 등록 절차(제32조) : 공공기관만 해당



- ✓ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관에 등록변경 사항의 검토 및 적정성 판단을 요청한 후, 상위 관리기관의 확인을 받아 개인정보보호 종합지원시스템(intraprivacy.go.kr)에 등록하여야 함
- ✓ 교육청 및 각급 학교 등의 개인정보 보호책임자는 교육부에 등록변경 사항의 검토 및 적정성 판단을 요청한 후, 교육부의 확인을 받아 등록하여야 함



2. 개인정보의 안전한 관리

🔒 개인정보 보호 인증(제32조의2)

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
- 경영진 차원에서 상시 모니터링 체계 구축
- 개인정보 침해사고에 효율적 대응 가능
- 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



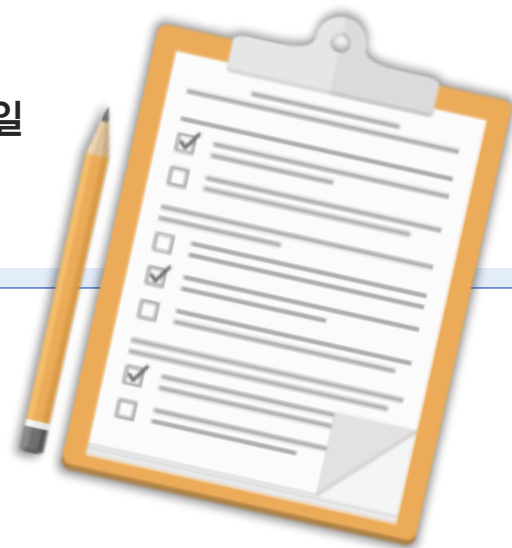


2. 개인정보의 안전한 관리

개인정보 영향평가(제33조) : 공공기관만 해당

▶ 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**로써 연계 결과 **50만명 이상의 정보주체**에 관한 개인정보가 포함되는 개인정보파일
- ✓ 구축·운용 또는 변경하려는 개인정보 파일로서 **100만명 이상의 정보주체**에 관한 개인정보파일



개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



2. 개인정보의 안전한 관리

🔒 개인정보 유출 통지 등(제34조) → 통지

▶ 적용 조항

법 제34조(개인정보 유출 등의 통지·신고), 시행령 제39조(개인정보 유출 통지의 방법 및 절차)

▶ 정의

[개정] 개인정보 유출 등: 개인정보가 분실·도난·유출

▶ 통지 요건

(1명 이상의 정보주체의) 개인정보가 유출 등이 되었음을 알게 되었을 때

▶ 통지 기한

[개정] 유출사실을 알았을 때 지체없이 – 정당한 사유가 없는 한 72시간 이내 (영 제39조 제1항)

[개정] [예외] 72시간이 넘어 통지할 수 있는 경우

✓ 유출 등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출 등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 통지 가능(영 제39조 제1항)

▶ 통지 방법

- [개별 통지(서면 등의 방법)]
- [예외] 연락처가 없으면 30일 이상 인터넷 홈페이지에 게시 (인터넷 홈페이지가 없으면, 사업장 등 보기 쉬운 장소에 30일 이상 게시)

▪ [개정 전] 유출 → [개정 후] 유출 등(분실·도난·유출)

▪ [개정 전] 24시간 이내(정보통신서비스 제공자 등), 5일 이내(일반 개인정보처리자) → [개정 후] 72시간 이내



2. 개인정보의 안전한 관리

🔒 개인정보 유출 통지 등(제34조) → 통지

▶ 통지 내용

다음 5가지를 정보주체에 통지

1. 유출 등이 된 개인정보의 항목
2. 유출 등이 된 시점과 그 경위
3. 유출 등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

[통지 내용 예외] 위 1 또는 2를 파악하지 못한 경우, 파악한 것과 3~5를 먼저 정보주체에 통지(우선 통지)하고, 나머지는 파악한 즉시 통지(추후 통지)

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



2. 개인정보의 안전한 관리

🔒 개인정보 유출 통지 등(제34조) → 신고

▶ 적용 조항

법 제34조(개인정보 유출 등의 통지·신고), 시행령 제40조(개인정보 유출 등의 신고)

▶ 정의

개인정보 **유출 등**: 개인정보가 **분실·도난·유출**

▶ 신고 요건

- 개인정보 유출 등이 되었음을 알게 되었을 때 다음 중 하나에 해당하는 경우(영 제40조 제1항)
 1. 1천 명 이상의 정보주체에 관한 개인정보가 유출 등이 된 경우
 2. **[신설]** 민감정보, 고유식별정보가 유출 등이 된 경우
 3. **[신설]** 외부로부터의 불법적인 접근에 의해 개인정보가 유출 등이 된 경우 //해킹에 의한 개인정보 유출
- **[신설]** [예외] 신고하지 않을 수 있는 요건 정의
 - ✓ 개인정보 유출 등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮은 경우

▶ 신고 기한

[개정] 유출사실을 알았을 때 지체없이 - 정당한 사유가 없는 한 72시간 이내 (영 제40조 제1항)

- ✓ 72시간이 넘어 신고할 수 있는 예외 규정은 없음

▶ 신고 내용

통지 내용과 동일, 신고 내용 예외도 통지 내용 예외와 동일

▶ 신고처

개인정보보호위원회 또는 한국인터넷진흥원



2. 개인정보의 안전한 관리

🔒 공공시스템 운영기관의 개인정보 안전성 확보 조치

[신설] 개인정보의 안전성 확보조치 기준(고시) 제3장 공공시스템 운영기관 등의 개인정보 안전성 확보조치(제14조~제17조)

- 일반적인 안전조치 이외에 공공시스템 운영기관이 추가로 지켜야 할 사항 명시
- 공공시스템: 다음에 해당하는 개인정보처리시스템 중 개인정보보호위가 지정한 시스템
 1. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 단일 시스템을 구축하여 다른 기관이 접속하여 이용할 수 있도록 한 단일접속 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우
 - 가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템
 - 나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템
 - 다. 정보주체의 사생활을 현저히 침해할 우려가 있는 민감한 개인정보를 처리하는 시스템
 2. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 표준이 되는 시스템을 개발하여 다른 기관이 운영할 수 있도록 배포한 표준배포 시스템으로서 대국민 서비스를 위한 행정업무 또는 민원업무 처리용으로 사용하는 경우
 3. 기관의 고유한 업무 수행을 지원하기 위하여 기관별로 운영하는 개별 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우
 - 가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템
 - 나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템
 - 다. 「주민등록법」에 따른 주민등록정보시스템과 연계하여 운영되는 시스템
 - 라. 총 사업비가 100억원 이상인 시스템
- 공공시스템 운영기관: 공공시스템을 운영하는 공공기관

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



2. 개인정보의 안전한 관리

🔒 공공시스템 운영기관의 개인정보 안전성 확보 조치

공공시스템 운영기관의 내부 관리계획 수립·시행(제15조)

1. **관리책임자 지정***에 관한 사항(영 제30조의2 제4항)
2. 관리책임자의 역할 및 책임에 관한 사항
3. 개인정보취급자의 역할 및 책임에 관한 사항
4. 제4조 제1항 제4호부터 제6호까지 및 제8호에 관한 사항
5. 제16조 및 제17조에 관한 사항

공공시스템 운영기관의 접속기록의 보관 및 점검(제17조)

- ✓ 접속기록 등을 **자동화된 방식으로 분석**하여 불법적인 개인정보 유출 및 오용·남용 시도 탐지하고 그 사유를 소명 등 필요한 조치
- ✓ **공공시스템 이용기관**이 소관 개인정보취급자의 접속기록을 직접 점검할 수 있는 기능 제공

공공시스템 운영기관의 접근 권한의 관리(제16조)

- ✓ 접근권한 관리는 인사정보와 연계.
- ✓ 인사정보에 등록되지 않은 자는 계정 발급 불가. 불가피하면 발급 내역에 기록하고 발급 가능
- ✓ 계정 발급 시 개인정보보호 교육 시행, 보안서약서 징구
- ✓ 정당한 취급자에게만 접근권한이 부여됐는지, 접근권한 변경 내역을 반기별 1회 이상 점검
- ✓ 공공시스템 이용기관은 위 조치 수행

* **시행령 제30조의2**(공공시스템 운영기관 등의 개인정보 안전성 확보 조치 등)

④ 공공시스템운영기관은 공공시스템별로 **해당 공공시스템을 총괄하여 관리하는 부서의 장을 관리책임자로 지정**하여야 한다.

3

개인정보 보호법 법령 해석 사례





3. 법령 해석 사례

🔒 개인정보 수집·이용 분야

▶ 서비스 품질에 대한 고객만족도 조사를 하면서 고객의 동의없이 개인정보를 이용해도 되는지요?

- ✓ (민간) 고객으로부터 동의를 받거나 계약체결의 이행을 위하여 필요한 범위 내에서 동의를 받지 않고 만족도 조사가 가능함
(공공) 법령에 근거해 민원인의 동의를 받지 않고 만족도 조사가 가능함
 - 민간은 개인정보 보호법 제15조 제1항 제1호에 따라 정보주체의 동의를 받고 개인정보를 수집 이용할 수 있음
 - 또한 물건판매 또는 서비스 제공 등 계약과 관련한 만족도 조사는 정보주체의 계약 체결 및 이행을 위하여 불가피하게 필요한 범위 내에서 정보주체의 동의를 받지 않아도 개인정보 수집·이용할 수 있음
 - 공공의 경우, 제15조 제1항 제3호에 따라 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우 동의를 받지 않고 개인정보를 수집 이용할 수 있음
 - 예를 들어 '공공기관의 운영에 관한 법률' 제13조에 따라 국민에게 직접 서비스를 제공하는 기관의 경우 매년 1회 이상 고객만족도 조사를 실시하여야 하며, '민원처리에 관한 법률' 제26조에 따라 행정기관의 장은 처리한 민원에 대하여 민원인의 만족 여부 및 개선사항 등을 조사하여 업무에 반영할 수 있음

KEY WORD

#고객만족도 조사, #제15조제1항제3호, #제15조제1항제4호



3. 법령 해석 사례

개인정보 수집·이용 분야

- ▶ 인터넷으로 서비스를 하는 회사입니다. 우리 회사는 홈페이지 회원가입 시 이용자로부터 동의를 받아 이름, 휴대폰 번호를 수집 및 저장하고 있습니다. 또한 SNS 계정을 통한 간편 회원가입 기능을 제공하고 있습니다. 이 과정에서 SNS 회사로부터 이용자의 이름, 휴대폰 번호, 이메일 주소를 제공받고 있습니다. 그런데 SNS 회사에서 받는 개인정보에 대해서는 이용자의 동의를 받지 않고, 우리 회사의 개인정보 처리방침에서 그 사실을 명시하고만 있습니다. SNS 회사에서 개인정보를 제공받는 것이 개인정보보호법에 위배되는지 궁금합니다.

✓ 정보주체의 동의를 받지 않고 SNS 회사에서 개인정보를 제공받아 이용하는 것은 개인정보보호법을 위반하는 것입니다.

- 일반적인 개인정보처리자는 「개인정보 보호법」 제15조 제1항 제1호에 따라, 정보주체에게 수집·이용되는 개인정보를 명확하게 알리고 동의를 받아야 하며, 이 때 동의의 방법은 법 제22조에 따릅니다.
- 따라서, 본인의 회사에서 정보주체에게 동의를 받은 내용 이외에 추가 개인정보를 제3자로부터 제공받을 때에는 별도의 동의를 받아야 하며, 별도의 동의없이 개인정보 처리방침에 기재하여 알리는 것만으로는 법 위반에 해당합니다.

KEY WORD

#SNS를 통한 개인정보 수집, #동의방법, #SNS 간편회원가입,

개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



3. 법령 해석 사례

🔒 개인정보 수집·이용 분야

- ▶ 교수로 재직 중인 사람의 사진, 성명, 성별, 출생연도, 직업, 직장, 학력, 경력 등의 개인정보를 해당 교수가 재직 중인 학과 홈페이지 등을 통해 수집하여 별도의 사이트에서 유료로 제공할 수 있는 지 궁금합니다.

- ✓ 학과 홈페이지 등에 자발적으로 공개된 개인정보를 수집하여 유료로 제3자에게 제공한 행위는 정보주체의 동의가 있었다고 객관적으로 인정되는 범위 내이므로 유료 등 영리 목적으로 제공하여도 정보주체의 별도 동의를 받지 않아도 됨
- 정보주체가 직접 또는 제3자를 통하여 이미 공개한 개인정보는 공개 당시 정보주체가 자신의 개인정보에 대한 수집이나 제3자 제공 등의 처리에 대하여 일정한 범위 내에서 동의를 하였다고 할 것임
 - 공개된 개인정보를 객관적으로 보아 정보주체가 동의한 범위 내에서 처리하는 것으로 평가할 수 있는 경우에도 동의의 범위가 외부에 표시되지 아니하였다는 이유만으로 또다시 정보주체의 별도의 동의를 받을 것을 요구한다면 이는 정보주체의 공개의사에도 부합하지 않고 정보주체나 개인정보처리자에게 무의미한 동의절차를 밟기 위한 비용만을 부담시키는 결과가 됨
 - 추가로 「개인정보 보호법」 제20조는 공개된 개인정보 등을 수집처리하는 때에는 정보주체의 요구가 있으면 즉시 개인정보의 수집 출처, 개인정보의 처리 목적, 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실을 정보주체에게 알리도록 규정하고 있으므로 공개된 개인정보에 대한 정보주체의 개인정보자기결정권은 이러한 사후통제에 의하여 보호 받게 됨
 - 따라서 이미 공개된 개인정보를 정보주체의 동의가 있었다고 객관적으로 인정되는 범위 내에서 수집·이용·제공 등 처리를 할 때는 정보주체의 별도 동의는 불필요하다고 보아야 하고, 별도의 동의를 받지 아니하였다고 하여 「개인정보 보호법」 제15조나 제17조를 위반한 것으로 볼 수 없음
 - 정보주체의 동의가 있었다고 인정되는 범위 내인지는 공개된 개인정보의 성격, 공개의 형태와 대상 범위, 정보주체의 공개 의도 내지 목적뿐만 아니라, 정보처리자의 정보제공 등 처리의 형태와 정보제공으로 공개의 대상 범위가 원래의 것과 달라졌는지, 정보제공이 정보주체의 원래의 공개 목적과 상당한 관련성이 있는지 등을 검토하여 객관적으로 판단하여야 함

KEY WORD

#정보주체 이외로의 수집, #공개된 개인정보, #공개된 목적과의 관련성, #정보주체의 동의



3. 법령 해석 사례

🔒 개인정보 수집·이용 분야

- ▶ 방호직으로 근무하고 있는 사람입니다. 방호직의 특성상 근무중 순찰을 실시하는데 관리자가 공개적인 게시판에 순찰보고서라는 항목으로 해당근무자의 성명, 순찰포인트(순찰 위치), 누락여부 등을 기재하여 게시하고 있습니다. 개인정보 보호법 위반이 아닌지요?

- ✓ 개인정보 보호법 제2조 제1호가 규정하는 개인정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보이며, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함합니다.
- 따라서, 법인 또는 단체의 이름(상호), 소재지 주소 및 전화번호, 업무별 연락처, 영업실적 등 전적으로 법인 또는 단체에 관한 정보는 개인정보에 해당하지 않습니다.
 - 반면, 개인사업자의 상호명, 사업장 주소, 전화번호, 사업자등록번호, 매출액 등 사업체 운영에 관한 정보는 원칙적으로 개인정보에 해당하지 않으나, 대표자 성명을 비롯한 임원진과 업무 담당자의 이름, 개인 연락처, 사진 등은 법인이나 단체에 관한 정보이면서 동시에 상황에 따라 개인정보로 취급될 수 있습니다.
 - 결국, 회사 순찰근무자의 순찰 현황은 법인에 대한 정보이면서 개인정보로 취급될 수도 있어 내부 공개가 위법이라고 단정하기 어려우나 공개하는 경우 성명의 일부를 알아볼 수 없도록 처리함이 바람직합니다.

KEY WORD

#개인정보의 정의, #법인정보, #직원 개인정보, #내부공개



3. 법령 해석 사례

개인정보 수집·이용 분야

- ▶ 개인정보 보호법에 따라 개인 사업자가 주민등록증을 수집할 수 없는 것으로 알고 있습니다만, 혹시 어느 정도 수집할 수 있는지요? 예를 들면 이름, 주민등록번호 앞자리, 주민등록번호 첫 번째 뒷자리, 발행일, 주민등록기관, 사진 중에서.

✓ 이름, 생년월일, 성별, 발행일, 주민등록기관, 사진은 주민등록번호가 아니므로 동의를 받아 수집할 수 있음

- 「개인정보 보호법」 제24조의2에 따라 개인정보처리자는 법률 등에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우 등 외에는 주민등록번호를 처리할 수 없음
- 이 때 주민등록번호란 주민등록법 제7조의2에 따라 시장·군수 또는 구청장이 주민에게 개인별로 고유한 등록번호를 부여한 것으로 생년월일, 성별을 포함한 13자리의 번호임
- 따라서 이름, 생년월일, 성별, 발행일, 주민등록기관, 사진은 주민등록번호가 아니므로 동의를 받아 수집할 수 있음

KEY WORD

#개인정보 수집이용 동의서, #주민등록번호, #주민등록증



3. 법령 해석 사례

🔒 개인정보 목적 외 이용·제공 분야

- ▶ 기관 내부에서 자체감사를 위하여 소속 직원의 개인정보를 처리할 수 있는지, 있다면 어떤 조건에서 처리할 수 있는지 궁금합니다.

- ✓ 당해 기관이 국가기관 등 공공기관 직원인지, 민간기관인지에 따라 다릅니다. 공공기관은 동의 없이 소속 직원의 개인정보를 수집·처리할 수 있지만, 민간기관은 소속 직원의 동의가 필요합니다.
 - '공공감사에 관한 법률' 제20조 제1항과 제3항은 자체감사를 위하여 공무원 및 소속 직원에게 자료 제출을 요구할 수 있다고 규정하고 있으므로, 다른 법률에 특별한 규정있는 경우에 해당하며, 이에 따라 공공기관은 동의없이 자체감사를 위하여 소속직원의 개인정보를 처리할 수 있음
 - (민간기관인 경우) 민간기관(회사 등)은 「개인정보 보호법」 제18조 제2항 제1호에 따라 소속 직원의 동의를 받거나 노사협의를 통해 자체감사를 위하여 개인정보를 수집, 이용하거나 가지고 있는 개인정보를 목적 외 이용 가능함

KEY WORD

#자체감사, #목적외 이용제공 #제18조제2항제1호, #제18조제2항제2호



3. 법령 해석 사례

🔒 고정형 영상정보처리기기(CCTV) 분야

- ▶ 아파트 입구 대로변에서 불법 유턴 차량이 많아 사고 위험이 있어 당 아파트에서 불법 유턴 차량을 신고할 목적으로 CCTV를 설치해도 되는지 문의 드립니다. 공동주택관리법 시행규칙 제8조 3항에 의거하여 관리주체는 보안 및 방범 목적 외의 용도로 활용하거나 타인에게 열람하게 하거나 제공하여서는 아니된다고 명시 되어 있어 아파트에서 설치하여 대로변 불법차량을 파악하여 신고 목적용으로 설치하여도 되는지 문의 드립니다.

✓ 아파트 관리사무소에서 불법 유턴 차량 신고 목적으로는 공개된 장소에 CCTV를 설치할 수 없음

- 「개인정보 보호법」제25조 제1항에 따라 누구든지 공개된 장소에는 법령에서 구체적으로 허용하고 있는 경우, 교통단속을 위하여 필요한 경우, 교통정보의 수집분석 및 제공을 위하여 필요한 경우 등의 목적으로 영상정보처리기기(CCTV)를 설치운영할 수 있음
- 따라서, 아파트 관리사무소에서 불법 유턴 차량 신고 목적으로는 공개된 장소에 CCTV를 설치할 수 없음
- 참고로, 교통단속을 위하여 CCTV를 설치하려면 설치목적에 부합하는 단속 권한이 있는 자가 설치하여야 함

KEY WORD

#CCTV, #교통정보 수집분석, #단속목적, #CCTV 설치목적 #단속권한



3. 법령 해석 사례

🔒 고정형 영상정보처리기기(CCTV) 분야

- ▶ 아파트 입주민이 본인 이외 특정시간대 승강기 내부 이용자의 상태를 확인하기 위하여 영상정보 열람 등을 요구하고 있으며, 관리사무소에서는 동의가 필요한 사항으로 경찰관 입회 하에 검색이 가능하다고 통보하고 있는데, 적절한 처리인지요?

✓ 정보주체의 동의를 받지 않은 상태에서 경찰관 직무집행법을 근거로 경찰 입회하에 영상정보를 열람할 수 없음

- 「개인정보보호법」 제35조 제1항에 따라 정보주체는 자신의 개인정보 열람을 해당 영상정보처리기기운영자에게 요구할 수 있으며, 같은 법 제18조 제2항에 따라 정보주체로부터 동의를 받은 경우 등에는 개인정보를 목적 외 이용하거나 제3자에게 제공할 수 있음
- 따라서, 관리사무소는 해당 CCTV 영상에 수록된 정보주체의 동의를 받아 열람을 허용하되, 관리사무소에서 관련 영상을 먼저 확인 후 해당 부분에 대해서만 열람하도록 하여 열람을 필요 최소한으로 제한해야 함
- 한편, 경찰이 「경찰관 직무집행법」 제8조 제1항 따른 사실확인을 하기 위해 현장에 입회한 사실만으로 정보주체의 동의를 받지 않은 제3자에게 영상정보를 열람하도록 할 근거는 되지 않음

KEY WORD

#CCTV, #제3자 제공(열람), #경찰의 CCTV 열람



3. 법령 해석 사례

🔒 고정형 영상정보처리기기(CCTV) 분야

- ▶ CCTV 열람 신청 시 모자이크 처리 비용의 주체가 누구인지 알고 싶습니다. 신청인 부담인지, CCTV운영 담당기관 부담인지 답변 부탁드립니다

✓ 열람에 드는 비용은 열람요구자가 부담함

- 「개인정보 보호법」 제35조 제1항 및 표준 개인정보 보호지침 제44조 제1항에 따라 정보주체는 영상정보 처리기기 운영자가 처리하는 개인영상정보에 대하여 열람 또는 존재확인 등을 해당 운영자에게 요구할 수 있도록 하였고, 이러한 요구를 받은 운영자는 지체없이 필요한 조치를 취해야 함
- 영상정보 처리기기 운영자는 사전에 공개한 열람절차와 방법에 따라 열람을 실시하되, 정보주체 이외의 자의 개인영상정보를 알아볼 수 없도록 모자이크 등 비식별조치를 취한 후 열람물을 제공해야 함
- 한편, 보호법 시행령 제47조에 개인(영상)정보처리자는 개인정보 열람요구를 한 정보주체에게 필요한 실비의 범위에서 비용을 청구할 수 있도록 하였으므로 열람요구자가 비용을 부담함
- 참고로, 시중에 보급된 비식별조치 프로그램을 활용하여 열람비용을 최소화하도록 권고함

KEY WORD

#CCTV, #열람비용, #모자이크



3. 법령 해석 사례

🔒 개인정보 목적외 이용·제공 분야

- ▶ 소속 공무원의 출장 여비 및 초과근무수당의 부당수령 등에 대한 제보나 의심 정황 발생 시, 제보 내용의 진위여부를 확인하기 위해 청사에 방호 목적으로 설치된 CCTV 영상정보를 이용할 수 있는지?

- ✓ **민간은 소속 직원의 동의 또는 노사협의를 통해 처리할 수 있으나, 공공기관은 공공 감사법에 근거하여 청사의 CCTV 영상을 자체감사에 이용할 수 있음**
 - '(공공)「개인정보 보호법」 제18조 제2항 제2호에 따라 법률의 특별한 규정이 있는 경우 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외 이용하거나 제3자에게 제공할 수 있음
 - '공공감사법 제20조 제1항, 제3항은 자체감사를 위하여 공무원 및 소속 직원에게 자료제출을 요구할 수 있다고 규정하고 있어, 다른 법률에 특별한 규정에 해당하며, 공공기관이 청사관리 목적으로 설치하여 수집한 CCTV 영상정보를 자체감사 목적으로 이용할 수 있음. 다만, 이 경우에도 다른 정보주체 등의 이익을 부당하게 침해하지 않도록 하여야 함
 - (민간기관인 경우) 「개인정보 보호법」 제18조 제2항 제1호에 따라 정보주체의 동의를 받아 개인정보를 목적외 이용 및 제3자 제공할 수 있으므로 소속직원으로부터 동의를 받아 CCTV 영상정보를 자체감사에 이용할 수 있으며, 노사협의를 통해 처리할 수 있음

KEY WORD

#자체감사, #목적외 이용제공, #CCTV, #제18조제2항제1호, #제18조제2항제2호



3. 법령 해석 사례

개인정보 파기 분야

- ▶ 민원인이 지방자치단체에서 보유하고 개인정보 수집에 대한 동의의 철회를 주장하며 그 파기를 요구하고 있습니다. 현재 보유하고 있는 개인정보를 파기하여야 하는지 궁금합니다.

✓ 지방자치단체에서 보유하고 있는 개인정보의 수집·이용 근거가 법령에 기반한 것이 아니라 정보주체의 동의에 기반한 것이라면 파기하여야 합니다.

- 「개인정보 보호법」 제4조 제4호는 정보주체에게 '개인정보의 파기를 요구할 권리'를 인정하고 있으므로, 정보주체는 개인정보의 파기를 요구할 수 있습니다.
- 단, 지방자치단체에서 보유하고 있는 개인정보의 수집·이용 근거가 「개인정보 보호법」 제15조 제1항 제2호, 제3호 '법령에 기반한 것'인 경우는 파기할 필요가 없습니다.

※ 다른 법령에서 그 개인정보가 수집대상으로 명시되어 있는 경우 그 삭제를 요구할 수 없음

KEY WORD

#정보주체의 권리보장, #개인정보의 파기, #타 법령과의 관계



3. 법령 해석 사례

개인정보 파기 분야

- ▶ 회원관리 시스템에서 회원 탈퇴 시, 이름, 연락처, 주소 등 개인을 식별하는 정보는 모두 지체 없이 파기합니다. 이때, 생성정보였던, 회원번호 000001도 함께 파기하여야 하는 것일까요? 회원번호 신규 생성 등을 위하여 회원번호만 따로 순차적으로 관리하려 합니다.

☒ 개인을 식별할 수 없는 숫자는 개인정보가 아니므로 파기 불필요.

- 「개인정보 보호법」 제21조 제1항에 따라 개인정보처리자는 다른 법령에 따라 보존하여야 하는 경우 이외에는 보유기간이 경과하거나 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때 지체 없이 그 개인정보를 파기하여야 함
- 따라서, 개인정보의 처리 목적이 달성된 경우 개인을 식별할 수 있는 정보(이름, 연락처, 주소 등)는 모두 지체 없이 파기해야 함
- 다만, 법 제58조의2에 따라 이 법은 시간비용기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보에는 적용하지 아니함
- 따라서, 관련정보가 모두 파기되어 연계 생성된 회원번호를 더 이상 누구의 개인정보인지 알아볼 수 없다면 이는 익명 정보로서 파기하지 않아도 됨

KEY WORD

#개인정보의 범위, #개인정보의 파기, #회원번호



3. 법령 해석 사례

개인정보 파기 분야

- ▶ 회원가입 시 개인정보 보유기간에 대해 '회원탈퇴 즉시 삭제'로 고지하고 있으나, 쿠폰 부정사용 등 불량회원을 식별하기 위해 일부 개인정보를 탈퇴 후 1개월 동안 보존하고 있는 경우, 수집동의서에 회원탈퇴 후 1개월까지 보관이라 명시하고 동의를 받아야 할까요?

✓ 개인정보 추가보관에 대한 동의를 받아 추가로 보관할 수 있음.

- 「개인정보 보호법」 제21조 제1항의 다른 법령에 따라 보존하여야 하는 경우 이외에는 보유 기간이 경과하거나 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때 지체 없이 그 개인정보를 파기하여야 합니다.
- 개인정보 추가 보관에 대하여 사전동의를 받지 않은 회원이 탈퇴한 경우 지체 없이 해당 정보를 파기하여야 합니다.
- 다만 「개인정보 보호법」 제15조에 따라 회원 가입시 혹은 탈퇴 이전에 정보주체(회원)에게 개인정보의 보유 및 이용기간 등에 대한 동의를 받은 경우에는 해당 개인정보를 필요한 범위내 추가로 보관할 수 있습니다.

KEY WORD

#개인정보의 파기, #유효기간제 #추가보관, #개인정보 수집이용 동의서, #불량회원



3. 법령 해석 사례

🔒 개인정보 파기 분야

- ▶ 전자상거래법 시행령 제6조에 따라 대금결제 및 재화 등의 공급에 관한 기록: 5년 등 개인정보 보존기간을 정하고 관리하고 있습니다. 회원이 결제와 관련하여, 7년 전 기록에 대한 조회를 요청하는 경우가 있는데, 위 보존기간 이상 개인정보를 보존해도 되는지요?

✓ 고객에게 연장보존에 대한 동의를 받으면 연장하여 보존할 수 있음

- 「개인정보 보호법」 제21조 제1항에 따라 개인정보처리자는 다른 법령에 따라 보존하여야 하는 경우 이외에는 보유기간이 경과하거나 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때 지체 없이 그 개인정보를 파기하여야 함
- 법령에서 보존기간을 별도로 정한 경우 보존기간이 경과되면 지체없이 개인정보를 파기해야 하나, 법 제15조 제2항에서 정한 개인정보의 수집·이용 목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 고객에게 알리고 새로 동의를 받으면 연장하여 보존할 수 있음

KEY WORD

#개인정보의 파기, #연장보존 #법령의 보존기간, #개인정보 수집·이용 동의서



3. 법령 해석 사례

🔒 개인정보 파기 분야

- ▶ 온라인쇼핑몰을 운영하면서 각종 이벤트를 개최할 때 별도 본인인증이 없는 간편가입 회원도 ID별로 참여가 가능하도록 하자, 이를 악용하여 수백개의 ID를 생성하여 멤버십포인트를 적립 및 사용하는 회원이 있어 회원가입 동의를 받아 부정고객에 한해 개인정보를 '영구' 보존하면서 걸러내려고 하는데, 해도 괜찮은지요?

✓ 개인정보 영구 보존은 보존 기한이 없으므로 법에 위반됨

- 「개인정보 보호법」 제21조 제1항에 따라 개인정보처리자는 다른 법령에 따라 보존하여야 하는 경우 이외에는 보유기간이 경과하거나 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때 지체 없이 그 개인정보를 파기하여야 함
 - 따라서, 별도의 보존기간을 정하지 않은 경우 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때까지 보유한다는 형태의 동의를 구하면 되나, '영구 보존'은 이러한 기한이 없으므로 법에 위반됨
- ※ 공공기관은 「공공기록물 관리에 관한 법률」에 따라 개인정보를 영구 보존할 수 있음

KEY WORD

#개인정보의 파기, #영구보존, #보유기간, #처리목적 달성, #보유기간 경과, #개인정보 수집이용 동의서



3. 법령 해석 사례

개인정보 업무 위탁 분야

- ▶ 산업안전보건법상 사업주가 안전보건관리책임자 등에 대해 직무교육을 실시하도록 되어 있고, 교육기관에 수강신청서를 제출하도록 되어 있습니다. 이 경우 해당 교육을 진행하는 안전보건 교육기관(예: 대한산업안전협회)은 개인정보 처리 위탁사에 해당하는지요?

- ✓ '업무 위탁' 과 개인정보 '제3자 제공' 모두 개인정보가 다른 사람에게 이전하거나 다른 사람과 공동으로 이용하게 되지만, 업무 위탁은 개인정보처리자의 업무처리 범위 내에서 개인정보 처리가 행해지고 위탁자가 위탁자인 개인정보처리자의 관리·감독을 받으며, 제3자 제공은 제3자의 이익을 위해서 개인정보 처리가 행해지고 제3자가 자신의 책임 하에 개인정보를 처리하게 됩니다.
- 산업안전보건법에 따른 법정 위탁교육을 위해 개인정보처리자가 보유한 개인정보를 직무교육 기관이 처리하도록 위탁할 수 있으며, 이 경우 위수탁자 모두 법 제26조를 준수하여야 함

KEY WORD

#개인정보 처리위탁, #직무교육, #위수탁자 관리

부록

개인정보 관련 법령, 고시, 가이드라인 현황



개인정보의 안전한 관리와 개인정보 보호법 법령 해석 사례



(부록) 개인정보 관련 법령, 고시, 가이드라인 현황

🔒 개인정보보호 관련 가이드라인 현황

| No | 유관 가이드명 | 발행시기 |
|----|------------------------------------|------------|
| 1 | 가명정보 처리 가이드라인 개정 | 2024-02-05 |
| 2 | 공공·민간 고정형 영상정보처리기기 설치·운영 가이드 라인 | 2024-01-19 |
| 3 | 개인정보 법령해석 사례 | 매년 발행 |
| 4 | 개인정보 보호법 및 시행령 개정사항 안내 | 2023-12-29 |
| 5 | 개인정보보호 가이드라인(공공기관 편) | 2023-12-28 |
| 6 | 홈페이지 개인정보 노출방지 안내서 | 2023-12-19 |
| 7 | 개인정보보호 가이드라인(통계작성 편) | 2023-11-15 |
| 8 | 개인정보 유출 등 사고대응 매뉴얼 | 2023-10-16 |
| 9 | 개인정보 보호 가이드라인(온라인 경품행사편) | 2023-05-03 |
| 11 | 2022 가명정보 활용 우수사례집 | 2023-03-28 |
| 12 | 우리 기업을 위한 EU 일반 개인정보보호법(GDPR) 가이드북 | 2023-02-03 |
| 13 | 개인정보 보호 가이드라인(인사·노무편) | 2023-01-31 |
| 14 | 개인정보 영향평가 대가산정 가이드 및 계산기 | 2022-12-15 |
| 15 | 아동·청소년 개인정보 보호 가이드라인(2022.7. 제정) | 2022-07-22 |

| No | 유관 가이드명 | 발행시기 |
|----|---------------------------------|------------|
| 16 | 개인정보 처리방침 작성지침 | 2022-03-03 |
| 17 | 알기쉬운 개인정보 처리 동의 안내서 | 2022-03-03 |
| 18 | 소상공인을 위한 개인정보보호 핸드북 | 2022-02-18 |
| 19 | 공동주택 개인정보보호 상담사례집 | 2022-01-18 |
| 20 | 스마트도시 개인정보 보호 가이드라인 | 2021-12-31 |
| 21 | 긴급 상황 시 개인정보 처리 및 보호수칙 | 2021-10-28 |
| 22 | 생체정보 보호 가이드라인 | 2021-09-08 |
| 23 | 개인정보 보호법 표준 해석례 | 매년 발행 |
| 24 | 인공지능(AI) 개인정보보호 자율점검표(개발자·운영자용) | 2021-07-20 |
| 25 | 사회복지시설 개인정보보호 가이드라인 | 2021-01-04 |
| 26 | 약국 개인정보보호 가이드라인 | 2021-01-04 |

* 개인정보포털 → 자료 → 지침자료

https://www.privacy.go.kr/front/bbs/bbsList.do?bbsNo=BBSMSTR_000000000049

감사합니다



※ 본 교재의 저작권은 한국인터넷진흥원에 있으며 교육 목적 외 상업적 등의 목적으로 재편집 사용을 금합니다.