

개인정보보호 정보보안교육



| 개인정보취급자가 알아야 할 개인정보보호법



N
ew
진짜

마트한



CONTENTS

- NEW 이슈 탐방

1 나는 개인정보취급자?

2 관리받고 있나요?

3 개인정보취급자의 법적 위험과 대응 방안

- SMART 시큐의 노트



NEW 이슈 탐방



대학생인 A씨는 여름방학 기간에 B편의점에서 하루 8시간 동안 알바를 하고 있습니다.

B편의점에서 상품을 구매한 고객에게 이벤트를 한다고 하여 명함이나 휴대전화번호를 수집하고 있습니다.

알바생은 개인정보취급자인가?



01

나는 개인정보취급자?

- 개인정보 처리자

: 개인정보를 처리하는 사업자 또는 법인, 단체, 개인 (주로 사업자)

- 개인정보 취급자

: 개인정보 처리자의 지휘 감독을 받아 개인정보를 처리하는 임직원, 파견 근로자, 시간제 근로자 등

고객 개인정보 처리 업무	담당자
서비스 개발	기획자, 개발자, 테스터, DBA
서비스 운영	기획자, 개인정보 담당자, 서비스운영자
고객 응대	전화, 게시판, email 등 고객응대 담당자
IT운영	데이터베이스, 서버 운영자
가입자 처리	가입자 유치 및 처리 담당자
기술지원	유무선 기술지원 엔지니어
마케팅	텔레마케터

비(非)고객 개인정보 처리업무	담당자
임직원 정보 관리	인사, 재무 담당자
주주 관리	투자자 관리(IR) 담당자
기자 등 관리	홍보 업무 담당자
정부, 공공 대응	대관 업무 담당자
협력업체 관리	협력업체 관리, 협업 담당자
고객사 관리	영업 담당자

01

나는 개인정보취급자?

개인정보의 정의

“개인정보”란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보

- 살아있는 개인에 관한 정보

- ✓ 돌아가신 분의 개인정보는 개인정보가 아님. 다만 해당 정보로 살아있는 개인을 식별할 수 있으면 개인정보가 될 수 있음
- ✓ (예) B가 돌아가신 A의 휴대전화를 사용한다면, A의 휴대전화번호는 B를 식별하는 개인정보가 될 수 있음

- 개인(사람)에 관한 정보

- ✓ 반려견의 정보는 개인정보가 아님. 다만 해당 정보로 개인을 식별할 수 있으면 개인정보가 될 수 있음
- ✓ 법인에 관한 정보는 개인정보가 아님. 사업자 등록증에 대표자 이름이 나오는데, 일반적으로 개인정보가 아님. 이걸 가지고 개인을 식별하는 데 사용하면 개인정보가 될 수 있음

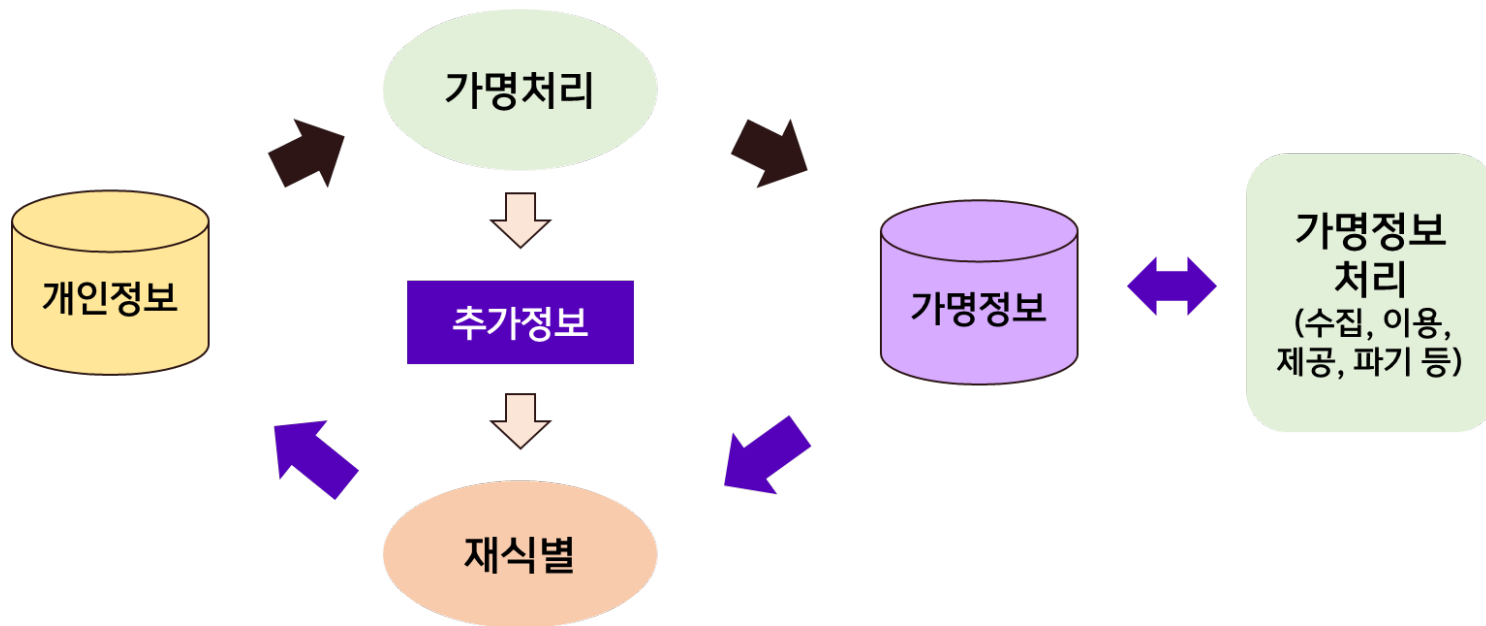
개인정보와 개인정보처리

- 식별정보 : 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
- 식별가능정보 : 해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 결합하여 알아볼 수 있는 정보
- 가명정보 : 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보
- 쉽게 결합하여 vs. 어렵게 결합하여?
 - ✓ 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보.
이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
 - ✓ 검색을 통해서 얻을 수 있는 정보
 - 이름 + 이메일주소
 - 이름 + 휴대전화번호
 - 이름 + 주소(시군구) + 주소(상세주소)

01 나는 개인정보취급자?

☒ 가명정보와 가명처리

- 가명처리: 개인정보를 식별 불가능하도록 처리 (예: 이름에서 * 처리)
- 재식별: 가명처리된 정보를 다시 식별할 수 있는 정보가 있을 경우 재식별 가능
- 법적 규제: 가명정보는 재식별을 최소화해야 하며, 추가 정보의 관리는 신중히 해야 함



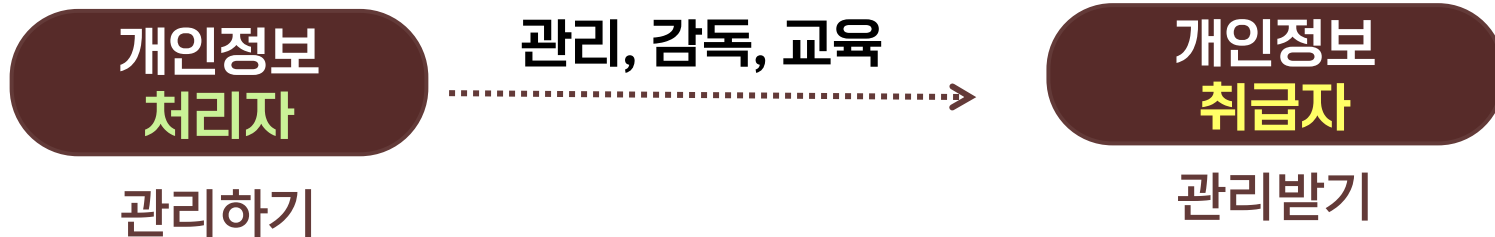
※ 개인정보보호법에서는 **가명정보 처리**에 **가명처리**를 포함해 설명하는 경우가 있음

02 관리받고 있나요?

개인정보보호책임자 (CPO: Chief Privacy Officer)

- 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로 개인정보처리방침에 명시되어 있음
- 회사의 개인정보 보호 총괄 책임자로 대부분의 회사는 개인정보 처리 방침을 통해 CPO 정보 공개
- CPO는 개인정보 취급자를 관리하고 교육할 의무가 있음

개인정보처리자의 3대 의무



02 관리받고 있나요?

관리

- 최소 계정, 최소 권한의 원칙: 개인정보처리시스템에 대한 접근 권한을 업무 수행에 꼭 필요한 사람에게만, 최소한의 권한만 부여, 유지
 - ✓ 계정: 꼭 필요한 개인정보취급자에게만 계정을 부여하여 개인정보취급자 수를 꼭 필요한 수만 운영
 - ✓ 권한: 읽기, 쓰기, 변경, 삭제, 다운로드 등 업무 수행에 필요한 최소 권한을 부여
- 1계정 1인 원칙(계정 공유 제한): 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 함
- 변경 관리: 업무 변경, 퇴사 등으로 접근 권한이 바뀌면, 지체 없이 개인정보처리시스템에 반영
 - ✓ 권한 부여, 권한 변경, 계정 삭제 등을 시행하고, 그 기록을 3년 이상 보관
- 일정 횟수 사용자 인증 실패 시 접근 제한: 일정 횟수 로그인 실패 시 차단, 비밀번호 재설정 등 필요한 조치 시행

02 관리받고 있나요?

감독

- 개인정보취급자가 개인정보보호법 등 관련 법규와 회사의 내부관리계획 등 개인정보보호정책을 준수하여 개인정보 업무를 수행하도록 감독
 - ✓ 서비스 기획 및 개발 등 개인정보 처리 업무 수행 시 개인정보 생명주기에서 개인정보가 안전하게 처리되는지 점검
- 개인정보의 분실·도난·유출·위조·변조·훼손 등 개인정보 사고가 발생하지 않도록 감독
 - ✓ 개인정보 유출 방지시스템 설치, 개인정보 암호화 등을 통해 개인정보 보호
- 개인정보 업무 처리 시 정보주체의 권리를 침해하지 않도록 감독

교육

- 개인정보 보호책임자 및 개인정보취급자를 대상으로 필요한 교육을 정기적으로 실시
 - ✓ 대상: 신규 입사자, 파견자, 시간제 근로자, 수탁사 인력 등

03 개인정보취급자의 법적 위험과 대응 방안

누설 금지 위반 사례

누구에게든지 집주소를 알려주지 말라는
입주민의 부탁을 받은 아파트 경비원이
찾아온 가족을 입주민의 집에 안내한 것이
개인정보를 누설·제공한 혐의로 30만 원 벌금형 선고

(한국아파트신문 2023.08.22)



- 개인정보보호법 제59조(금지행위)

- ✓ 개인정보를 처리하거나 처리하였던 자는 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.
- ✓ 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위

03 개인정보취급자의 법적 위험과 대응 방안

부당한 이용 금지 위반 사례

1심 재판부는 법률의 미비로 수능시험 고사장에서
수험생의 개인정보를 알아내 연락한 감독관에게
무죄를 선고 → **법 제59조 제3호에 ‘이용’ 추가**
(2023.9.15 시행)

(법률신문 2023.2.12)



- 개인정보보호법 제59조(금지행위)
 - ✓ 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위
 - ✓ 정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 이용, 훼손, 멸실, 변경, 위조 또는 유출하는 행위
- 제19조(개인정보를 제공받은 자의 이용·제공 제한)
 - ✓ 개인정보처리자로부터 개인정보를 제공받은 자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 아니 된다.

03 개인정보취급자의 법적 위험과 대응 방안

유출 금지 위반 사례

야근하는 모습을 영상으로 촬영하여
SNS에 올린 세무사가 게시물을 확대하니
고객의 개인정보가 보여 개인정보를 유출한 혐의로
2심에서 벌금형에 집행유예를 선고 받음

(머니투데이 2023.12.29)



- 개인정보보호법 제59조 (금지행위)

- ✓ 개인정보를 처리하거나 처리하였던 자는 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.
- ✓ 정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 이용, 훼손, 멸실, 변경, 위조 또는 유출하는 행위

03 개인정보취급자의 법적 위험과 대응 방안

대응 방안_1. 최소한의 권한으로 업무하기

- 업무를 하는 데 반드시 개인정보를 다룰 필요가 있지 않다면, 개인정보취급자가 되지 않겠다고 하는 것이 좋음
- 개인정보취급자가 되더라도 특정한 화면과 항목만 열람만 할 수 있는 등 개인정보에 대한 접근 권한을 최소로 갖는 것이 바람직함

대응 방안_2. 업무 후 개인정보 잊기

- 전·현직 개인정보취급자뿐 아니라 누군가의 개인정보를 “업무상 알게 된” 분들은 업무를 하지 않을 때는 개인정보에 관해서는 잊어버리는 것이 좋음
- 법원의 판단은 다를 수 있으므로 친구나 지인을 만나 업무에서 다뤘던 개인정보 이야기는 아예 꺼내지 않아야 함

대응 방안_3. 개인정보 관련 법규 학습

- 개인정보보호 담당 부서에 자신의 업무와 관련된 구체적인 개인정보보호 교육을 요청
- 개인정보보호법 등 관련 법령을 공부하고, 사례를 들어 구체적으로 이해하려고 노력
- 나아가 자신의 업무에 관한 여러 법령을 찾아보고 공부하는 것도 시도

03 개인정보취급자의 법적 위험과 대응 방안

최소한의 권한으로 업무

죄형 법정주의

- ✓ 범죄와 형벌은 **미리 법률에 규정**되어야 함
- ✓ 범죄의 성립과 처벌은 **행위 시의 법률**에 따른다((형법 제1조(범죄의 성립과 처벌) 제1항))

고의범의 처벌

- ✓ 죄의 성립요소인 **사실을 인식하지 못한 행위**는 벌하지 아니한다.
다만, 법률에 특별한 규정이 있는 경우에는 예외로 한다(형법 제13조(고의))

과실범의 처벌

- ✓ 정상적으로 기울여야 할 주의(注意)를 게을리하여 죄의 성립요소인 **사실을 인식하지 못한 행위**는 법률에 특별한 규정이 있는 경우에만 처벌한다(형법 제14조(과실))

양벌 규정

- ✓ 어떤 범죄에 대해 **행위자와 함께 그 행위자와 일정한 관계가 있는 타인(자연인 또는 법인)에 대해서도 형을 부과**하도록 한 규정
- 보통 **관리, 감독의 책임**이 있는 자
- ✓ 어떤 법인의 대표자나 법인 또는 개인의 대리인·사용인·종업원이 위법행위를 한 경우 벌칙 규정을 적용받아 처벌되는 것은 실제 행위를 한 자인데,
그 위반행위에 따라 이익 등을 얻고 있는 자는 그 법인 또는 사용주이므로 법인 또는 사용주가 위반 행위를 방지하거나 예방 조치를 할 책임이 있다고 봄



SMART 시큐의 노트



나는 개인정보취급자?

- 개인정보취급자는 개인정보처리자의 지휘·감독 아래 고객 및 비고객 정보를 처리하는 모든 임직원, 시간제 근로자 등을 포함
- 개인정보처리자의 지휘·감독 아래 개인정보를 처리하는 자로 정규직, 계약직, 시간제 근로자, 파견직 등 고용 형태와는 관계없음



관리받고 있나요?

- 개인정보처리자는 취급자의 계정과 권한을 최소화하고, 계정 공유를 금지하며, 시스템 접근 제한과 변경 이력을 관리
- 개인정보취급자로서 적절한 교육과 관리·감독을 받는 것은 개인정보보호를 위한 중요한 기반임



개인정보취급자의 법적 위험과 대응 방안

- 개인정보취급자는 최소한의 권한만 유지하고, 업무로 알게 된 개인정보를 외부에 누설하거나 부당하게 사용하지 않도록 함
- 법적 책임을 피하기 위해 개인정보보호법과 관련 규정을 숙지하고 준수하는 노력이 필요

개인정보보호 정보보안교육

| 개인정보보호법 개정에 따른 제도의 변화



노트

New
진짜

마트한



CONTENTS

- NEW 이슈 탐방

1 의료·통신으로 확장되는 마이데이터사업

2 N차 수탁자까지 관리하라고?

3 세계 최초 개인정보 처리방침 평가제

- SMART 시큐의 노트



NEW 이슈 탐방



개인정보보호법 개정

- 2023년 3월, 개인정보보호법 전면 개정, 2011년 법 제정 이후 변화가 가장 많았음
- 2023년 9월 , 2024년 3월과 9월, 개정 규정이 단계별로 시행되고 있음
- 법률에 따라 새로운 제도가 생기면, 그것이 우리 사회에 적용되고 정착하는 데 시간이 걸림
- 이번 강의에서는 법 개정예 따라 신설되거나 보완되는 제도를 설명하고자 함



금융권의 마이데이터사업

- 2020년 8월 시행, 신용정보법에 ‘본인신용정보관리업’이 도입되면서 마이데이터사업 시행
- 신용정보법 제2조(정의)
 - ✓ “본인신용정보관리업”이란 개인인 신용정보주체의 신용관리를 지원하기 위하여 신용정보를 (대통령령으로 정하는 방식으로) 통합하여 그 신용정보주체에게 제공하는 행위를 영업으로 하는 것(제9호의2)
 - ✓ “본인신용정보관리회사”란 본인신용정보관리업에 대하여 금융위원회로부터 허가를 받은 자 (제9호의3)

01 의료·통신으로 확장되는 마이데이터사업

전송 요구권

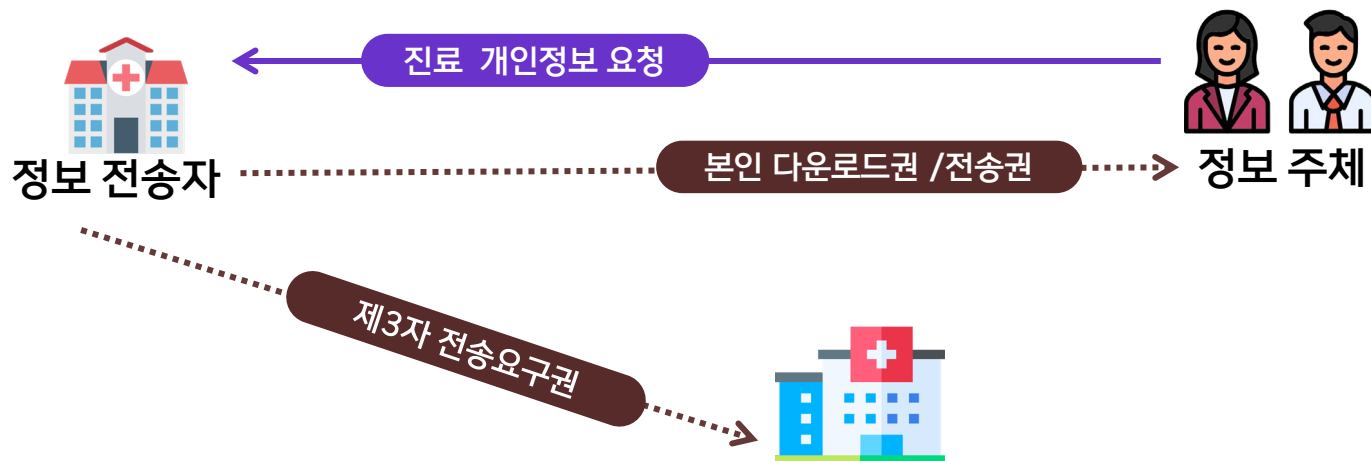
- 정보주체가 개인정보처리자에게 자신에 관한 개인정보를 본인 또는 ‘개인정보관리 전문기관’(마이데이터사업자) 또는 다른 개인정보처리자에 전송해 달라고 요구할 수 있는 권리
- 여러 산업과 분야에서 마이데이터사업을 진행할 수 있는 법적 근거 마련



01 의료·통신으로 확장되는 마이데이터사업

전송 요구권의 종류

- **본인 전송 요구권**: 정보주체가 개인정보처리자에게 자신에 관한 개인정보를 정보주체 본인에게 전송해 달라고 요구
 - ✓ 개인정보처리자: 개인정보 처리 능력 등을 고려하여 대통령령으로 정하는 기준에 해당
- **제3자 전송 요구권**: 정보주체가 개인정보처리자에게 자신에 관한 개인정보를 ‘개인정보관리 전문기관’ 또는 다른 개인정보처리자(일반수신자)에 전송해 달라고 요구
 - ✓ 개인정보처리자: 매출액, 개인정보의 보유 규모, 개인정보 처리 능력, 산업별 특성 등을 고려하여 대통령령으로 정하는 기준에 해당



01

의료·통신으로 확장되는 마이데이터사업

전송 요구 대상 개인정보

- 정보주체의 동의를 얻어 수집한 개인정보(민감정보, 고유식별정보 포함)
(제15조 제1항 제1호, 제23조 제1항 제1호 또는 제24조 제1항 제1호)
- 필수정보: 정보주체와의 계약 체결 또는 계약의 이행을 위해 수집한 개인정보
(제15조 제1항 제4호)
- 개인정보위가 전송 대상으로 의결한 개인정보



01 의료·통신으로 확장되는 마이데이터사업

개인정보관리 전문기관의 업무

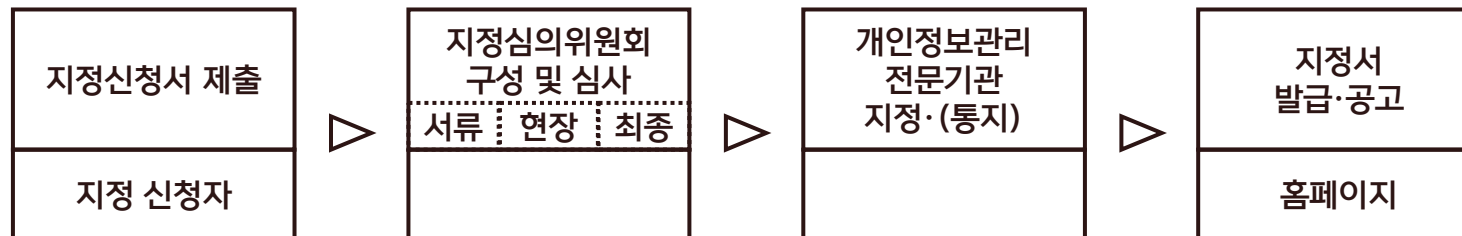
- 개인정보의 전송 요구권 행사 지원
- 정보주체의 권리행사를 지원하기 위한 개인정보 전송시스템의 구축 및 표준화
- 정보주체의 권리행사를 지원하기 위한 개인정보의 관리·분석

개인정보관리 전문기관

- 일반 전문기관: 전송받은 개인정보를 관리·분석하여 통합조회, 맞춤형 서비스, 연구, 교육 등에 이용하는 업무를 수행하는 자
- 특수 전문기관: 의료정보 등을 관리·분석하여 통합조회, 맞춤형 서비스, 연구, 교육 등에 이용하는 업무를 수행하는 자
- 중계 전문기관: 일반적인 정보수신자가 아니라, 개인정보 전송 중계에 필요한 시스템 운영 및 기능을 제공하는 업무 및 정보전송자의 전송을 지원하는 업무를 수행하는 자
- 일반수신자: 전송 요구권을 통해 수신한 정보를 단순 확인 목적으로만 사용하는 자

● ‘개인정보관리 전문기관’ 지정심사 절차

- 지정권자: 개인정보위 또는 관계 중앙행정기관의 장
- 지정심사: 개인정보관리 전문기관이 지정요건(기술수준 및 전문성, 안전성 확보조치 수준, 재정능력 등)을 확인하는 심사
- 지정절차: 지정신청 서류 접수 → 서류 검토 → 현장실사 → 종합심사 → 지정 통지, 지정서 발급·공고
- 지정 유효기간은 3년, 전문기관 재지정 시 심사를 통한 재지정



01 의료·통신으로 확장되는 마이데이터사업

‘일반수신자’ 등록 절차

- **등록의무:** 개인정보 보호법 제35조의2항에 따라 정보를 수신받으려는 일반수신자는 개인정보위의 개인정보 전송지원 플랫폼에 등록 후 정보 수신
- **등록절차:** 일반수신자가 개인정보 전송 지원 플랫폼 등록 신청시 개인정보위는 일반수신자의 시설 및 기술 기준 등 확인·검토 진행

‘일반수신자’ 등록 절차

- **의료:** 불필요한 CD·서류 발급없는 환자 진료 서비스를 구현하고 의료데이터 기반의 바이오·헬스 신시장 창출로 산업경쟁력 강화
- **통신:** 국민의 합리적인 통신소비 선택을 촉진하고 문화·여가·안전 등 타 분야의 데이터와 결합한 융합서비스를 통해 국민 편익 제고

01 의료·통신으로 확장되는 마이데이터사업

마이데이터사업의 주요 이슈

개인정보 전송 요구권 vs 마이데이터사업

- 정보주체의 전송 요구권보다 마이데이터사업 자체에 초점
- 개인정보관리 전문기관 및 일반수신자가 프라이버시 보호에 필요한 자격 요건을 갖춰야 함

전송 요구권은 전송 데이터 범위 선택부터 보장되어야 함

- Privacy by Default 원칙의 적용
- 개인이 선택할 수 있는 전송 개인정보 범위 확대, 보장
 - ✓ 민감성이 높은 정보만 정보주체가 전송정보의 범위를 직접 선택?
- 전송 변경, 중단, 파기 등의 정보주체의 권리 보장

01

의료·통신으로 확장되는 마이데이터사업

마이데이터사업의 주요 이슈

프라이버시 보호 대책

- 보안 측면 - 데이터 분산 vs 데이터 집중
- 정보수신자의 IT보안, 정보보호 관리체계 요건 필요
- 마이데이터사업 참여자에 대한 철저한 관리, 감독, 위반 시 제재 필요

02 N차 수탁자까지 관리하라고?

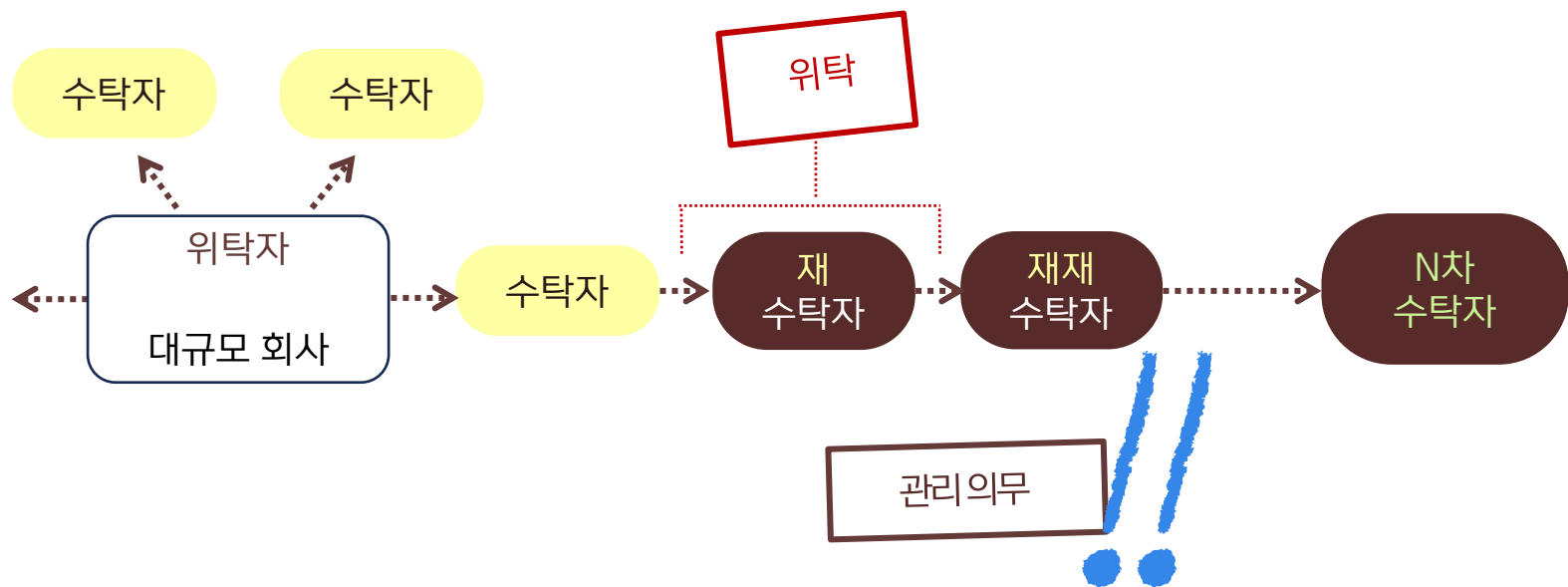
개인정보 처리 (업무) 위탁(법 제26조)

- 위탁: 개인정보 처리(업무)를 제3자에게 맡김
 - ✓ 수집, 이용 등 개인정보의 처리를 위탁하거나 개인정보 처리가 포함된 업무를 위탁
 - ✓ 재위탁: 위탁받은 개인정보 처리업무를 제3자에게 다시 위탁함
 - ✓ 재수탁: 개인정보 처리업무를 재위탁받음
- 위탁자: 개인정보 처리업무를 위탁하는 개인정보처리자
- 수탁자: 개인정보 처리 업무를 위탁받아 처리하는 자
- 재수탁자: 개인정보 처리업무를 위탁받아 처리하는 자로부터 위탁받은 업무를 다시 위탁받은 제3자
 - ✓ [개정] 수탁자에 재수탁자가 포함됨
 - 수탁자에 N차 수탁자까지 포함

02 N차 수탁자까지 관리하라고?

수탁자, 재수탁자, 재재수탁자?

- 개인정보 처리 위탁: IT 외주, 고객센터, 클라우드 서비스, 상품 배송 등
개인정보 처리 업무를 다른 기업에 위탁하는 것. 다른 기업에 위탁하지만,
개인정보 처리 업무가 포함되지 않으면, 개인정보 처리 위탁은 아님.
- 이론적으로 수탁자(1차), 재수탁자(2차), 재재수탁자(3차), N차 수탁자(N차)까지 생길 수 있음



02 N차 수탁자까지 관리하라고?

위탁자의 책임과 의무

- 수탁자 선정 시 개인정보보호 역량 고려
- 문서로 계약 – 법령에서 정한 내용을 포함(제1항)
- 수탁자 관리, 감독의 의무(제4항)
- 위탁 사실(수탁자, 위탁업무 내용) 공개(제2항)– 개인정보 처리방침
- 홍보, 판매 권유 업무 위탁 시 정보주체에게 개별 알림(제3항) – ‘서면 등의 방법’(영 제17조 제5항). 바뀌면 지체없이 다시 알림
- 수탁자는 수탁 업무를 제3자에게 다시 위탁하려는 경우에는 위탁자의 동의를 받아야 함
- 손해배상 책임 – 수탁자의 법 위반으로 발생한 손해에 관한 배상책임은 위탁자에 있음(제7항)

02 N차 수탁자까지 관리하라고?

위탁자의 수탁자 관리·감독 의무(제26조 제4항)

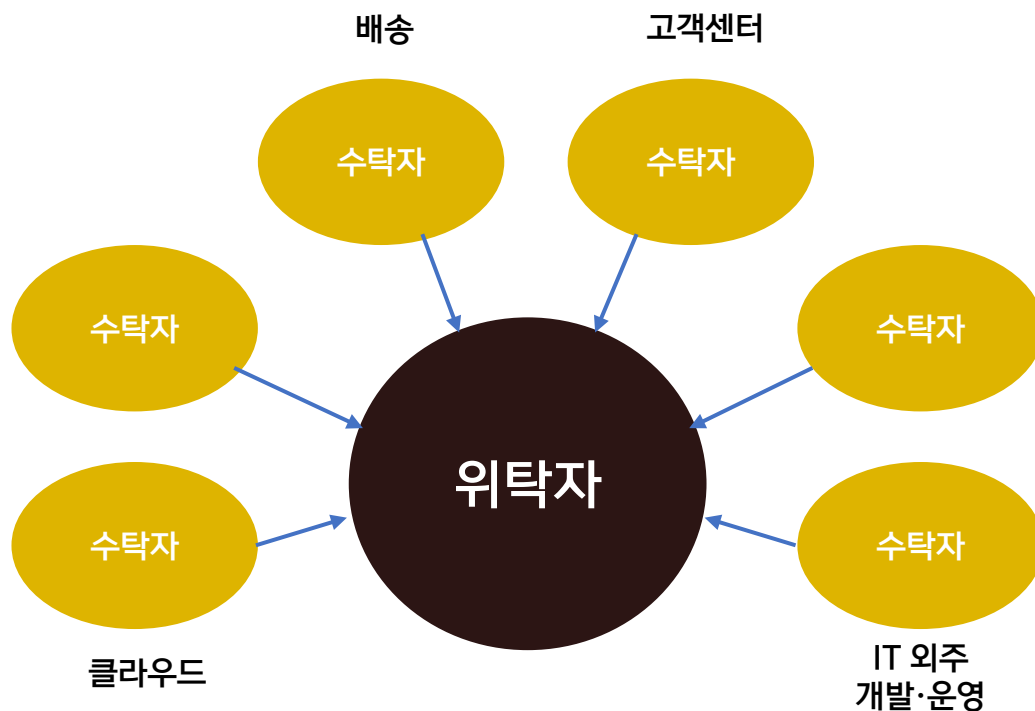
- 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
- 개인정보의 기술적·관리적 보호조치에 관한 사항 – 개인정보의 안전성 확보조치 기준 준수
- 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육
- 재위탁 제한에 관한 사항 – 재위탁 시 (최초) 위탁자의 동의 필수
- 개인정보의 관리 현황 점검 등 감독
- (참고) 수탁자의 의무는 위탁자의 의무를 역으로 보면 됨

02 N차 수탁자까지 관리하라고?

위탁자 vs. 수탁자

- 전통적 위·수탁 모델: 소수 대형 위탁자-다수 소형 수탁자

→ 수탁자 및 정보주체에 대한 책임을 대형 위탁자에 물음



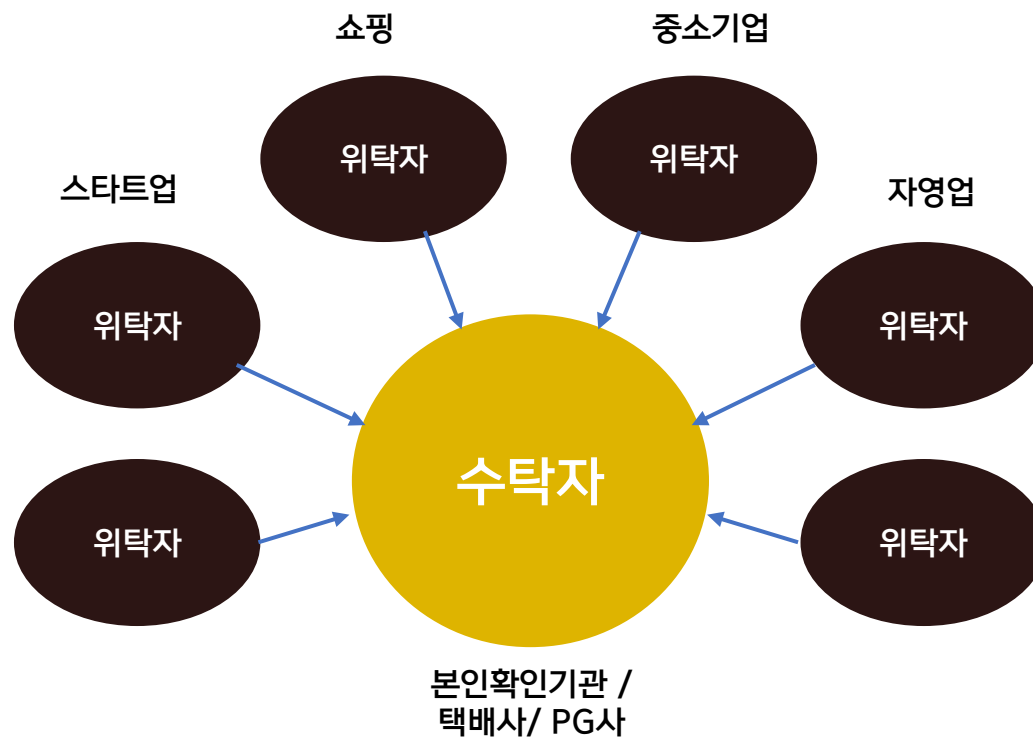
[위·수탁 모델]
소수 대형 위탁자-다수 소형 수탁자

02 N차 수탁자까지 관리하라고?

위탁자 vs. 수탁자

- 새로운 위·수탁 모델: 다수 소형 위탁자-소수 대형 수탁자

→ 수탁자의 개인정보보호 역량이 위탁자보다 좋을 수 있음



[위·수탁 모델]
다수 소형 위탁자-소수 대형 수탁자

02 N차 수탁자까지 관리하라고?

대형 수탁자에 대한 (소형) 위탁자의 의무 수행 방법

- 개인정보보호 인증을 받은 수탁자 선정
- 계약 시 법적 의무가 포함된 계약서 요청
 - ✓ 개인정보위에서 제시한 표준계약서 이용
- 수탁자에 관리, 감독, 교육 증빙(증적) 요청
 - ✓ 대부분의 대형 수탁자는 해당 활동을 하고, 관련 증빙을 준비해 두고 있음
 - ✓ 필요 시 요청했다는 증빙 준비 – 이메일 등
- 외국 수탁자에게는 국내 개인정보보호법을 준수해야 한다는 점을 고지

02 N차 수탁자까지 관리하라고?

개인정보보호법에 따른 수탁자의 법적 의무

- 개인정보의 수집, 이용, 제3자 제공, 목적 외 이용제공 제한, 파기, 개인정보취급자 관리감독, 안전조치 의무, 가명정보처리 특례, 개인정보 처리방침, 개인정보보호 책임자 지정, 정보주체의 권리 보장, 개인정보취급자의 금지 의무 등 개인정보처리자에 적용되는 대부분의 규정이 적용됨
- 적용되지 않는 규정은 손해배상책임(제39조), 법정손해배상의 청구(제39조의2) 극히 일부에 불과하므로, 개인정보처리자로서 책임감을 갖고 법 의무를 준수하면서 개인정보를 처리해야 함
 - ✓ 수탁자의 법 위반으로 발생한 손해배상책임은 위탁자가 계약서에 포함시키거나 위탁자가 정보주체에 손해배상을 한 뒤 수탁자에 구상권을 행사하는 방식으로도 배상 의무가 발생할 수 있다는 점에 유의

03 세계 최초 개인정보 처리방침 평가제

개인정보 처리방침

개인정보보호법 제30조(개인정보 처리방침의 수립 및 공개)에 따라 개인정보처리자가 반드시 갖춰야 할 문서

처리의
투명성·책임성

- ✓ 개인정보 생명주기에 따른 보호 업무 수행 및 법규 준수

처리방침
평가제

- ✓ 적정성, 가독성, 접근성 기준에 따른 평가

커뮤니케이션
수단

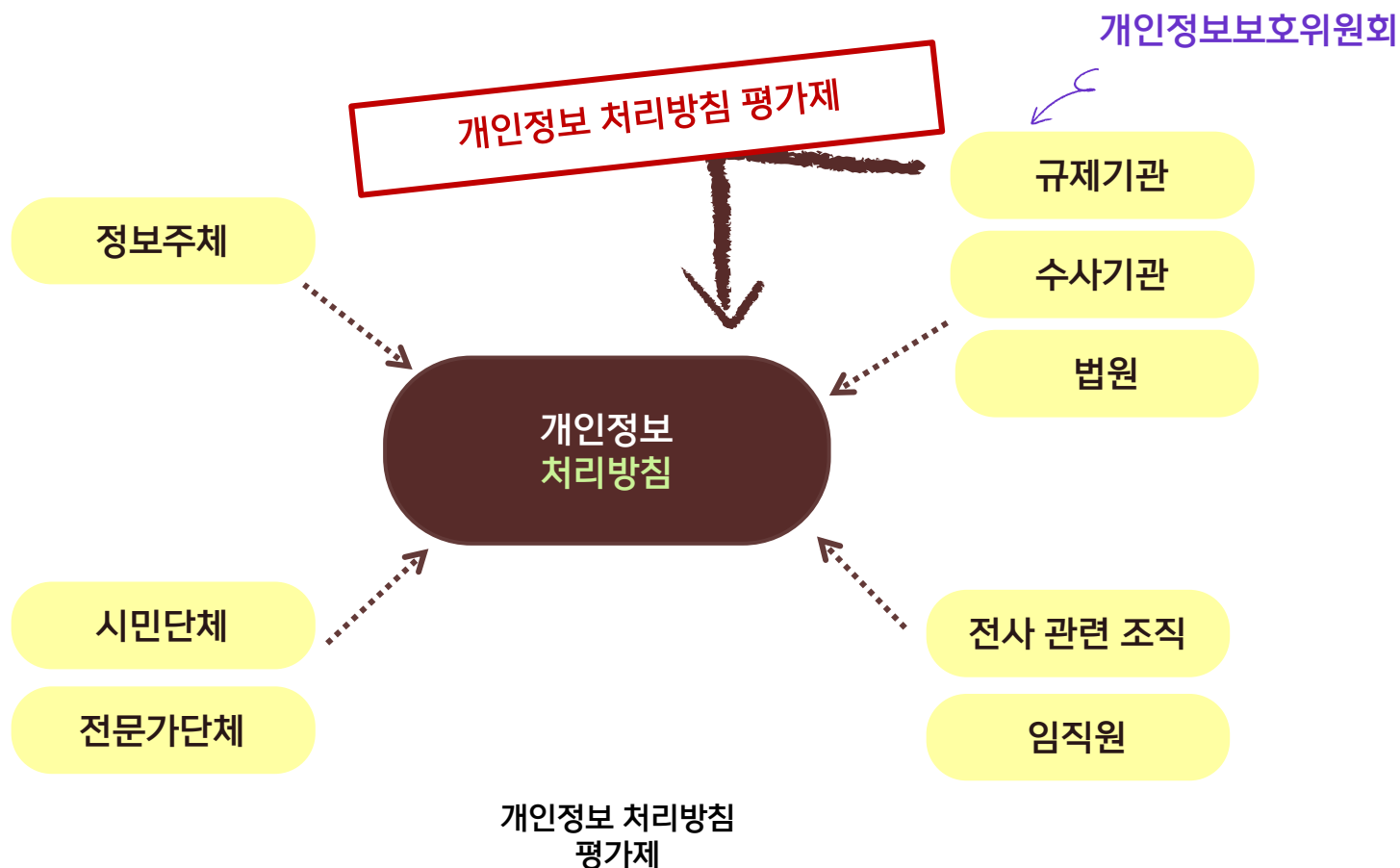
- ✓ 정보주체 등 이해관계자와의 커뮤니케이션

동의의
같음

- ✓ 국외 개인정보 처리 위탁·보관

03 세계 최초 개인정보 처리방침 평가제

개인정보 처리방침의 이해관계자



02 N차 수탁자까지 관리하라고?

평가제의 취지

- 개인정보 처리방침에 대한 평가와 개선을 통해 개인정보 처리의 투명성과 책임성 강화
- 개인정보 처리방침 상 개인정보 처리의 적정성, 정보주체 권리보장 정도 등을 평가하여 개인정보 보호 수준 개선 유도

평가 기준

- 적정성: 법령에 따라 기재해야 할 내용을 포함하는지, 그 내용이 적정한지 여부
- 가독성: 개인정보 처리방침을 **알기 쉽게 작성**하였는지 여부
- 접근성: 개인정보 처리방침을 정보주체가 **쉽게 확인할 수 있는 방법**으로 공개하는지 여부

02 N차 수탁자까지 관리하라고?

평가 기준 및 지표 - 26개 항목, 42개 지표

- **적정성(19개 항목)**

- ✓ **적합성(8개):** 필수·권장 기재 사항 작성 여부, 기재 내용의 법령 부합성 등
- ✓ **권리보장(5개):** 정보주체의 권리 보장을 위한 사항 기재 여부 등
- ✓ **안전성(6개):** 개인정보를 안전하게 관리하도록 추가적인 의무를 부여한 항목

- **가독성(4개 항목)**

- ✓ 처리방침의 구성 방법(줄 간격, 목차 등), 문장·어휘의 적정성 등

- **접근성(3개 항목)**

- ✓ 개인정보 처리방침의 공개 방식 등 정보주체가 처리방침을 쉽게 확인 및 접근할 수 있는지

- (참고) 평가 기준 및 지표는 평가제를 시행하면서 결과를 반영하며 일부 변경될 가능성 있음



SMART 시큐의 노트

✔ 의료·통신으로 확장되는 마이데이터사업

- 개인정보 전송 요구권으로 금융, 의료, 통신 등 다양한 산업에서 마이데이터 사업이 가능해짐
- 정보주체는 본인 데이터의 다운로드 요청과 제3자 전송을 요구할 수 있음
- 데이터 보안 문제를 방지하기 위해 정보보호 조치와 강력한 요건 마련이 필요함

✔ N차 수탁자까지 관리하라고?

- 수탁자 관리 범위가 재수탁자와 그 이상의 단계까지 포함되도록 확대됨
- 위탁자는 개인정보보호 역량을 고려해 수탁자를 선정하고, 계약 체결 시 보호 조치 내용을 포함해야 함
- 관리·감독을 위해 증빙 자료 요청, 개인정보 인증 활용 등 효율적인 방법을 사용할 수 있음

✔ 세계 최초 개인정보처리방침 평가제

- 개인정보처리방침 평가제는 적정성, 가독성, 접근성을 기준으로 개인정보처리자의 투명성을 평가
- 평가는 특정 요건을 충족하는 개인정보처리자에게만 적용되며, 필수 기재 사항 준수를 중점적으로 검토
- 정보주체와 이해관계자들이 쉽게 접근하고 이해할 수 있는 방침 작성이 요구됨