

개정 개인정보 보호법상

가명정보의 개념 및

가명처리에 관하여

고학수, 백대열, 구본효, 정종구, 김은수

「데이터 3법 시대의 과제: 가명처리, 연구목적 활용, 데이터 거래」 웨비나

개정 개인정보 보호법상

가명정보의 개념 및 가명처리에 관하여

고학수

서울대학교 법학전문대학원 교수

백대열

서울대학교 법학대학원 박사과정

구본효

서울대학교 법학대학원 박사과정

정종구

서울대학교 법학대학원 박사과정

김은수

서울대학교 아시아태평양법연구소

목 차

I. 서론

II. 개정 개인정보 보호법상 가명정보 및 가명처리의 개념

III. 가명정보의 보호

IV. 가명정보의 결합

V. 결론

I. 서론

I. 서론

‘데이터 3법’의 개정: 주요 내용

개인정보 보호법

- ① 개인정보 개념체계 **명확화**: 개인정보, 가명정보, (이른바) 익명정보
- ② **가명정보의 처리에 관한 특례** 도입
- ③ 목적합치의 원칙 도입
- ④ 감독·집행 권한과 조직을 개인정보 보호위원회로 최대한 일원화

신용 정보법

- ① **가명정보의 개념 및 그 이용·제공 등에 관한 특례** 도입
- ② 익명처리의 개념 및 데이터전문기관에 의한 적정성 평가·추정 제도 도입
- ③ 신용평가회사의 라이선스 세분화 ⑤ 본인신용정보관리업(MyData) 도입
- ④ 신용정보업의 업무범위 확대 ⑥ 금융분야에 새로운 개인정보 자기결정권 도입

정보 통신망법

동법에 규정되어 있던 개인정보 보호에 관한 사항들을 삭제하고
개인정보 보호법으로 이관

I. 서론

향후의 과제 및 본 연구의 목적

□ 개인정보 보호법은 개정되었으나...

- 이론적으로나 실무적으로나 많은 쟁점들이 등장할 것으로 예상됨
- 다수의 세부 내용들이 하위 법령이나 고시에 위임되어 있음
- 국무조정실 외, “개인정보 비식별 조치 가이드라인” (2016)의 후속조치?

□ 본 연구의 목적

- 개정 개인정보 보호법상 가명정보 및 가명처리의 개념 및 관련 쟁점 검토
- 가명정보의 보호를 위한 각종 조치(기술적·관리적 보호조치, TTP의 활용) 제언
- 가명정보의 결합 관련 쟁점 검토

II. 개정 개인정보 보호법상 가명정보 및 가명처리의 개념

II. 가명정보 및 가명처리의 개념

개인정보, 가명정보 및 가명처리, 익명정보

□ 개정 개인정보 보호법 제2조 제1호 및 제1의2호

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. **“개인정보”**란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.

가. 성명, 주민등록번호 및 영상 등을 통하여 **개인을 알아볼 수 있는 정보**

나. 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.

다. **가목 또는 나목**을 제1호의2에 따라 **가명처리함**으로써 **원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보**(이하 **“가명정보”**라 한다)

1의2. **“가명처리”**란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 **추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것**을 말한다.

II. 가명정보 및 가명처리의 개념

개인정보, 가명정보 및 가명처리, 익명정보

□ 개정 개인정보 보호법 제58조의2

제58조의2(적용제외) 이 법은 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보에는 적용하지 아니한다.

👁 (이른바) **“익명정보”**

□ 비교: 생명윤리 및 안전에 관한 법률 제2조 제19호

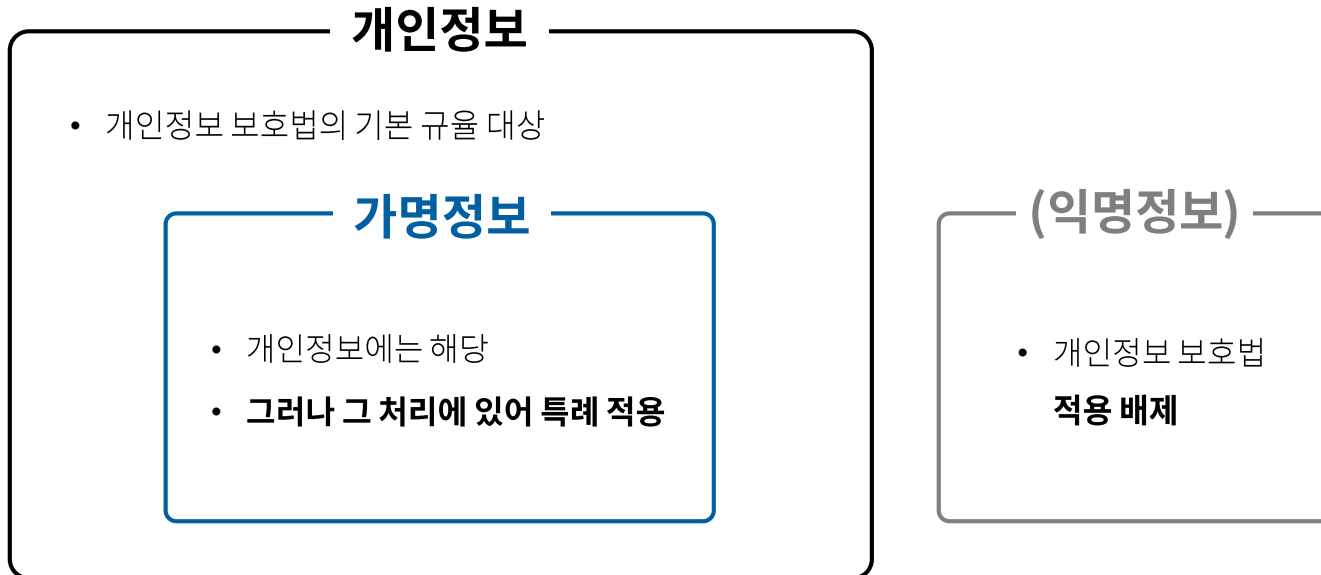
제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

19. **“익명화”(匿名化)**란 개인식별정보를 영구적으로 삭제하거나, 개인식별정보의 전부 또는 일부를 해당 기관의 고유식별기호로 대체하는 것을 말한다.

II. 가명정보 및 가명처리의 개념

개인정보, 가명정보 및 가명처리, 익명정보

□ 개념의 도해

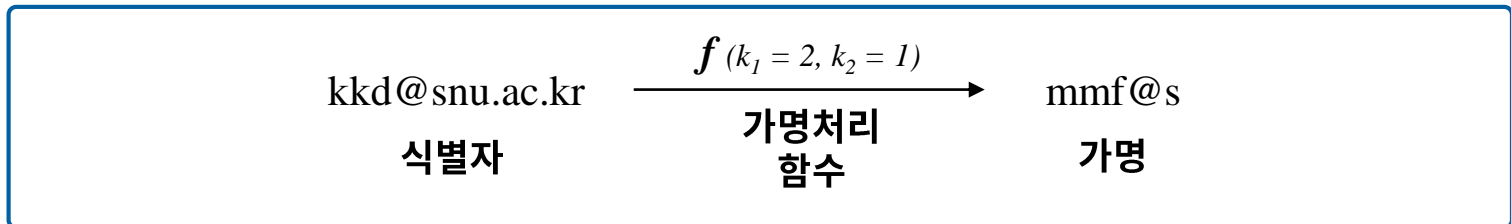


II. 가명정보 및 가명처리의 개념

가명처리의 기본 구조

□ 가명처리(pseudonymisation)

- 특정 정보주체를 식별할 수 있는 정보, 즉 **식별자(identifier)** 등의 정보에 대해,
- 그 중 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 만들어진 **가명(pseudonym)**을 대응시키는 것
- 따라서 이를 하나의 함수(function) 내지 사상(map)으로 이해할 수 있는바, 이를 강학상 **가명처리 함수(pseudonymisation function)**라 함



II. 가명정보 및 가명처리의 개념

가명처리의 기본 구조

□ 가명처리 비밀(pseudonymisation secret)

- ① 가명으로부터 원래의 식별자를 **복원**해낼 수 있도록 하는
- ② 가명처리 함수 관련 정보 일체
- 개정 개인정보 보호법상 “원래의 상태로 복원하기 위한 추가 정보”(제2조 제1호 다목)
- 암호화 키(key), 가명처리 매핑 표(pseudonymisation mapping table) 등 다양한 형태를 띠 수 있음.



$(k_1 = 2, k_2 = 1)$

암호화 키

식별자	가명
kkd@snu.ac.kr	mmf@s
kke@gmail.com	mmg@g
sapi@snu.ac.kr	ucrk@s
...	

가명처리 매핑 표

II. 가명정보 및 가명처리의 개념

가명처리의 기본 구조

□ 가명처리 비밀(pseudonymisation secret)

- 개정 개인정보 보호법 제28조의4 제1항
 - 개인정보처리자는 가명정보를 처리하는 경우에는 **원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등** 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.
- (참고) 이와 **구별**하여야 할 개념
 - **보조 정보(auxiliary information), 배경 지식(background knowledge)**
 - 가명처리 비밀이 아닌 정보로서 가명과 결합하여 원래의 식별자를 복원하는 등으로 정보주체를 재식별하는 데 사용될 수 있는 것들(식별자의 유형, 등장 빈도 등)
 - 법에 규정된 “추가 정보”가 보조 정보나 배경 지식을 포함하는지는 불분명함

II. 가명정보 및 가명처리의 개념

가명정보의 처리에 관한 특례

□ 개정 개인정보 보호법은 “제3장 개인정보의 처리”의 하위 항목으로

“제3절 가명정보의 처리에 관한 특례”를 신설함.

- 이 때 **“처리”**란 개인정보(가명정보)의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 포괄하는 용어임(개인정보 보호법 제2조 제2호 참조).

II. 가명정보 및 가명처리의 개념

가명정보의 처리에 관한 특례

□ 주요 내용

- 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 **정보주체의 동의 없이 가명정보를 처리**할 수 있음(개정 개인정보 보호법 제28조의2 제1항)
- 동법 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 **서로 다른 개인정보처리자 간의 가명정보의 결합**은 개인정보 보호위원회 또는 관계 행정기관의 장이 지정하는 **전문기관**이 수행하도록 함(동법 제28조의3 제1항)
- 개인정보처리자의 **가명정보에 대한 안전조치의무 등** 규정(동법 제28조의4)

II. 가명정보 및 가명처리의 개념

가명정보의 처리에 관한 특례

□ 주요 내용

- 누구든지 **특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니** 되며, 개인정보처리자는 **가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는** 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 함(동법 제28조의5)
- 위 각 의무 위반시 형사처벌, 과징금, 과태료 등의 **제재** 규정(동법 제28조의6 등)
- 개인정보 보호법의 **일부 규정 적용 배제** – 정보주체의 권리행사 일부 제한 (동법 제28조의7)

III. 가명정보의 보호

III. 가명정보의 보호

가명정보 보호의 필요성

□ 개인정보처리자의 가명정보 보호 의무

- 개정 개인정보 보호법은 기존에 제29조에서 개인정보처리자의 안전조치의무를 규정하고 있던 것에 더하여 제28조의4에서 **가명정보에 대한 안전조치의무를 추가로** 규정함

제28조의4(가명정보에 대한 안전조치의무 등) ① 개인정보처리자는 **가명정보를 처리하는 경우에는** 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 **안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.**

② 개인정보처리자는 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 **관련 기록을 작성하여 보관하여야 한다.**

III. 가명정보의 보호

가명정보를 어떻게 보호할 것인가?

- 유럽연합 일반 개인정보 보호법(General Data Protection Regulation; GDPR)
 - “기술적·관리적 조치(technical and organisational measures; TOM)”

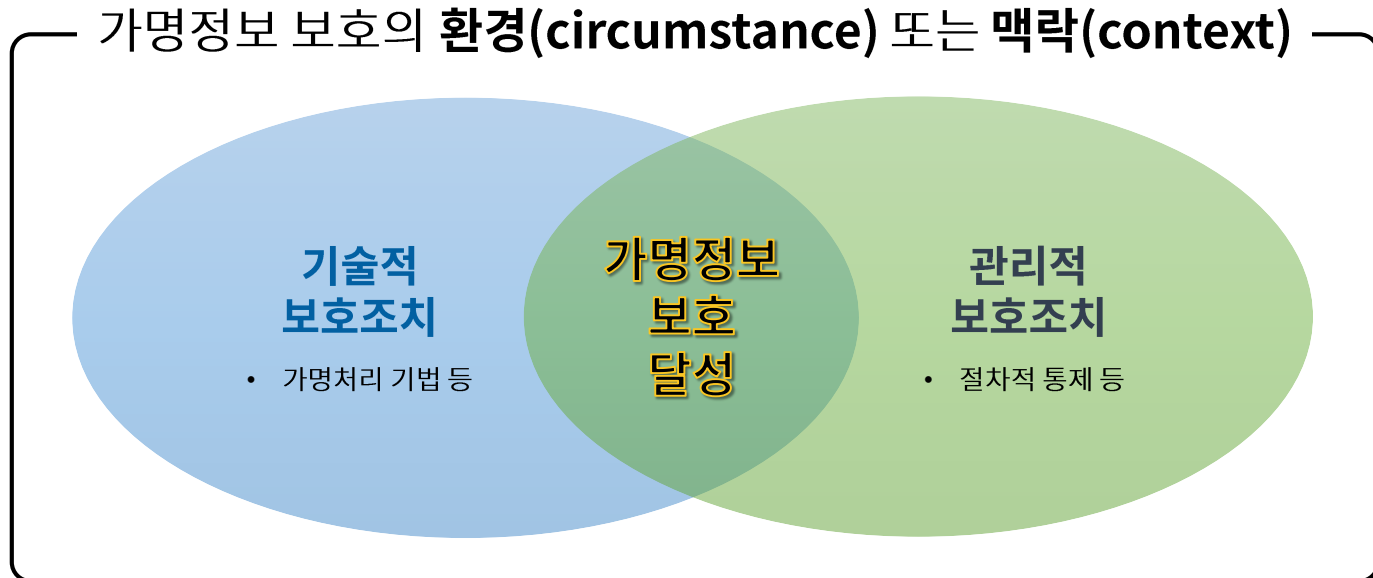
- 개정 개인정보 보호법
 - “기술적·관리적 및 물리적 조치”

- **가명정보의 보호조치 개관: 법이 정하고 있는 것과 그렇지 않은 것**
 - 1. 기술적 보호조치
 - 2. 관리적 보호조치
 - 내부통제와 외부감사
 - 신뢰할 수 있는 제3자(Trusted Third Party; TTP)의 활용

III. 가명정보의 보호

가명정보를 어떻게 보호할 것인가?

□ 가명정보의 보호 도해



III. 가명정보의 보호

가명정보를 어떻게 보호할 것인가?

□ 개정 개인정보 보호법에 명문의 규정은 없지만, 모든 개인정보처리자가 이러한 기술적·관리적 보호조치를 일괄적으로 동일하게 취해야 하는 것일까?

- ① 가명정보를 처리하는 개인정보처리자의 **유형** 내지 **규모**
- ② 해당 개인정보처리자가 실제로 처리하는 **가명정보의 개별적인 특성**
(특히 유출 등 사고 발생시 정보주체의 프라이버시에 초래될 수 있는 침해의 중대성)

☞ 앞서 설명한 가명정보의 **환경** 또는 **맥락!**

☞ 이러한 요소들을 종합적으로 고려하여 **보호조치의 구체적 내용에 차등**을 둘 수 있을 것임

☞ 개인정보처리자 또한 **개별 가명정보 처리 사안별 의사결정에 있어 이를 고려**할 수 있을 것

III. 가명정보의 보호

1. 기술적 보호조치

□ 가명처리 기법 선택시 고려해야 할 요소들

- 가명처리의 목적
- 가명처리에 따른 비용 및 예산상의 제약
- 가명정보의 유용성
- 가명처리 기법의 보안상 안전성

☞ 이 또한 가명정보 보호의 **환경** 또는 **맥락**을 형성하는 요소들

☞ **개별 사안별로** 이러한 요소들을 종합적으로 고려하여 **비교·형량**해야 할 것

III. 가명정보의 보호

2. 관리적 보호조치 - (1) 내부통제와 외부감사

□ 가명정보 관련 내부통제(internal control)의 구성요소 및 그 주요 내용(예시)

통제환경	가명정보 관련 내부통제와 그 중요성에 관한 지배기구 및 경영진의 태도와 의식 및 행동을 제고해야 함
위험평가 절차	자신이 보유한 가명정보에 대한 다양한 재식별 공격 시나리오들을 선제적으로 상정하여 그에 따른 위험을 파악 및 평가하고 그에 대한 대응책을 결정해야 함
정보시스템	개인정보취급자 개인별 로그(log) 기록 시스템을 운영하고, 가명정보의 처리 목적이 달성되거나 가명정보 보유 기간이 경과한 경우 이를 지체 없이 파기해야 함
통제활동	가명처리 관련 각종 승인을 담당하는 데이터심의위원회(data review board; DRB)를 내부적으로 설치하고, 물리적 통제절차를 마련하며, 업무를 분장해야 함
통제의 모니터링	가명정보 처리의 전 과정에 걸쳐 가명정보가 효과적으로 보호되고 있는지 여부를 지속적으로 평가해야 함(특히 최신 보안 및 공격 기술을 지속적으로 반영해야 함)

III. 가명정보의 보호

2. 관리적 보호조치 - (1) 내부통제와 외부감사

□ 가명정보의 맥락에서 외부감사(external audit)의 의의

- 내부통제를 아무리 효과적으로 설계·실행한다 하더라도 이는 그 특성상 일정한 한계를 가질 수밖에 없는바, 이러한 한계를 보완하는 데에는 외부감사가 효과적일 수 있음
- **개정 개인정보 보호법은 이에 관하여 명문의 규정을 두고 있지 않으나, 가명정보의 맥락에서 외부감사란 ‘가명정보의 생성, 저장, 보유, 가공, 편집 등 처리의 전 절차에 걸쳐 충분한 보호조치가 이루어지는 등으로 개인정보 보호법의 관련 규정들이 준수되었는지 여부를 개인정보처리자 외부의 독립된 감사인이 검증하는 절차’를 의미한다고 볼 수 있음**
- 자발적인 외부감사를 통해 가명정보를 보다 효과적으로 보호할 수 있을 것임

III. 가명정보의 보호

2. 관리적 보호조치 - (2) TTP의 활용

□ 신뢰할 수 있는 제3자(Trusted Third Party; TTP)의 활용

- 일반적으로 TTP란 ‘물리적 공간 및 조직적 구성 측면에서 데이터 처리자와는 **독립된 존재**’를 의미함
- 개인, 조직 모두가 TTP에 해당할 수 있음
- 가명정보의 보호에 있어서는 ① **원래의 식별자를 복원해낼 수 있도록 하는 가명처리 비밀에 대한 접근 권한과** ② **가명정보에 대한 접근 권한을 분리하는 것이 핵심인바,** 이를 위해 TTP를 활용할 수 있음
- TTP의 예: 의료 영역에서의 어니스트 브로커(honest broker),
개정 개인정보 보호법상 가명정보 결합전문기관(동법 제28조의3)

IV. 가명정보의 결합

IV. 가명정보의 결합

개정 개인정보 보호법에 따른 가명정보의 결합

- 일정한 요건 하에 **정보주체의 동의 없이도** 개인정보의 결합을 허용
 - ① **가명정보**에 한하여
 - ② **전문기관**을 통해서만 결합이 가능하도록 하고,
 - ③ 결합된 정보의 **반출**에도 일정한 제약을 가함

제28조의3(가명정보의 결합 제한) ① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 **서로 다른 개인정보처리자 간의 가명정보의 결합**은 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 **전문기관**이 수행한다.

② **결합을 수행한 기관 외부로 결합된 정보를 반출**하려는 개인정보처리자는 **가명정보 또는 제58조의2에 해당하는 정보로 처리한 뒤 전문기관의 장의 승인을 받아야** 한다.

IV. 가명정보의 결합

개정 개인정보 보호법에 따른 가명정보의 결합

□ 논의의 방향

- 향후 실무에 있어 복잡다단하면서도 중요한 쟁점들이 다수 등장할 것으로 예상됨
- 그러나 그 논의의 방향은 **향후 고시 등 하위법령 및 가이드라인에 구체적으로 어떠한 내용이 담기느냐에 따라** 크게 달라질 것임

제28조의3(가명정보의 결합 제한) ③ 제1항에 따른 결합 절차와 방법, 전문기관의 지정과 지정 취소 기준·절차, 관리·감독, 제2항에 따른 반출 및 승인 기준·절차 등 **필요한 사항은 대통령령으로 정한다.**

개인정보 보호법 시행령 일부개정령안(2020. 3. 31. 입법예고)

제29조의2(개인정보처리자 간 가명정보의 결합 등) ⑥ 제1항부터 제5항까지 규정한 사항 외에 가명정보 결합 절차와 방법, 반출 및 승인 등에 **필요한 세부사항은 [개인정보] 보호위원회가 정하여 고시한다.**

IV. 가명정보의 결합

개정 개인정보 보호법에 따른 가명정보의 결합

□ 논의의 방향

- 따라서 본 연구에서는 **향후 논의를 위한 전제**로서 다음의 **네 가지** 핵심 쟁점들을 제시하고, 이에 대하여 살펴보기로 함

1. ‘서로 다른’ 개인정보처리자 간 가명정보 ‘결합’의 의미

2. 가명정보 결합의 문제상황

3. 가명정보 결합의 실익

4. 가명정보 결합에 있어 전문기관의 지위와 역할

IV. 가명정보의 결합

1. ‘서로 다른’ 개인정보처리자 간 가명정보 ‘결합’의 의미

□ ‘서로 다른’ 개인정보처리자 간

□ 가명정보 ‘결합’의 의미

- 개정 개인정보 보호법은 가명정보 ‘결합’의 개념을 별도로 정하고 있지 않으나, 실무적·이론적으로 그 의미가 문제될 수 있음
- 가령, 서로 다른 유형의 가명정보를 ‘결합’한다는 것은?



영상 형태의 가명정보



+

이름	카드결제 내역	병원진료 내역
김갑동	5/1 A 10,000원	5/3 X병원
이을서	5/2 B 20,000원	5/2 Y병원

= ?

표 내지 문자열 형태의 가명정보

IV. 가명정보의 결합

1. ‘서로 다른’ 개인정보처리자 간 가명정보 ‘결합’의 의미

□ 가명정보 ‘결합’의 의미

- 가령, 행과 열로 구성된 하나의 표로 표현 가능한 **구조화된 데이터(structured data)**의 경우에도...

이름	쇼핑몰 ID	성별	구매내역
김갑동	kkdshop	남성	5/4 정장구두 A
이을서	eulseo	여성	5/2 운동화 B

구두를 판매하는 X회사의 고객 데이터베이스



이름	쇼핑몰 ID	연령대	구매내역
김갑동	kkdbagY	30대	4/28 서류가방 A
이을서	eulseo	20대	5/2 백팩 B

가방을 판매하는 Y회사의 고객 데이터베이스

- 이를 ‘**합쳐(combine, consolidate)**’ 더 큰 형태의 표를 만드는 것만 결합에 해당하는 것인지,
- 아니면 서로 다른 개인정보처리자 간 가명정보를 상호 비교하는 등 일종의 ‘**연결(link)**’ 행위까지 결합에 해당하는 것인지 **불분명함**

IV. 가명정보의 결합

2. 가명정보 결합과 관련된 리스크


- 어떠한 방식으로든 서로 다른 두 개인정보 데이터베이스를 ‘결합’하면,
 - 한편으로는 통계적 분석 등에 있어서의 활용도가 증대되지만,
 - 다른 한편으로는 정보량이 늘어남으로 인해 정보주체가 재식별되거나 프라이버시가 침해될 위험이 증가하게 되는 것이 일반적임.
 - 따라서 향후 가명정보 결합 관련 세부 쟁점들을 논함에 있어서는 **이러한 리스크 증대 현상 등을 면밀히 고려해야 함.**

- 리스크를 야기하는 주체에 따른 분류
 - ① 해당 가명정보를 보유하는 **개인정보처리자**에 의한 위험
 - ② **결합전문기관**에 의한 위험
 - ③ 해커 등 **잠재적인 제3의 공격자(motivated intruder)**에 의한 위험

IV. 가명정보의 결합

3. 가명정보 결합의 실익

□ 개인정보처리자가 가명정보의 결합으로 얻을 수 있는 편익은?

- 가명정보의 결합은 **무시할 수 없는 수준의 비용을 수반하기 마련**이므로, 비용-편익 분석이 필요함
- 가장 큰 잠재적 편익으로 생각해볼 수 있는 것은...
 - 결합된 가명정보를 토대로 **개인 맞춤형(targeted)** 서비스를 제공하고 마케팅을 실시
 - **그러나** 개정 개인정보 보호법상 이러한 행위가 허용되는지는 **불분명함**
 - ‘통계작성, 과학적 연구, 공익적 기록보존 등을 위한’ 것에 해당하는지 여부가 불분명함 (동법 제28조의3 제1항)
 - 나아가 가명정보의 결합은 그 자체로 개정 개인정보 보호법상 ‘처리’에 해당하는데, 앞서 살펴본 바와 같이 “누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리”하는 것은 금지됨(동법 제28조의5 제1항)  해석상 논란이 있을 수 있음

4. 가명정보 결합에 있어 전문기관의 지위와 역할

- 향후 실무적으로 결합전문기관의 지위와 역할이 문제될 가능성이 있음
- 전문기관의 지위와 역할에 관하여 상정할 수 있는 두 가지 모델

1. 소극적 전문기관 모델

- 전문기관의 역할을 수동적·제한적으로 파악하는 입장
- 전문기관의 역할은 각 개인정보처리자로부터 제공받은 가명정보를 단순히 결합하는 데 국한됨

2. 적극적 전문기관 모델

- 전문기관의 통제장치로서의 기능을 강조하는 입장
- 전문기관은 스스로의 판단에 따라 결합의 전 과정에서 각종 보호조치를 취할 수 있음

4. 가명정보 결합에 있어 전문기관의 지위와 역할

□ 두 모델 사이에서 어떤 선택을 하느냐에 따라...

- ① 가명정보 결합의 **절차와 방법**(특히 결합된 정보의 **반출** 방법)
 - ② 전문기관의 **지정 및 지정취소 기준**
(특히 순수 민간기관을 전문기관으로 지정할 것인지 여부)
 - ③ 전문기관에 대한 **관리·감독**
- ☞ 위 각 사항들에 관한 구체적 내용이 달라질 것임!

□ 개정 개인정보 보호법의 입장은?

- 개정 개인정보 보호법의 문언만으로는 분명하지 아니하나, 현재의 시행령 일부개정령안은 **적극적 전문기관 모델에 가까운 입장**을 취하고 있는 것으로 보임(동안 제29조의2 참조)

V. 결론

V. 결론

개정 개인정보 보호법: ‘끝’이 아닌 ‘시작’!

□ 오늘 발표를 통해 살펴본 내용들

- 개정 개인정보 보호법상 가명정보 및 가명처리의 개념 및 관련 쟁점
- 가명정보의 보호를 위한 각종 조치(기술적·관리적 보호조치, TTP의 활용)
- 가명정보의 결합 관련 쟁점

□ 앞으로 나아가야 할 방향

- 앞서 살펴본 바와 같이 이론적으로나 실무적으로나 많은 쟁점들이 등장할 것으로 예상됨
- 하위 법령, 고시, 가이드라인 등을 구체적으로 마련하는 한편, **관련 쟁점들에 대한 상세하고 진지한 논의를 통해 데이터 시대로의 변화에 적극적으로 대응할 필요가 있음**

질의 · 응답

감사합니다.