데이터 3법과 비식별화

데이터 3법과 비식별 기술 동향

2020. 7. 16

Halla Univ. in wonju
Dept. Computer Eng.
Soon Seok Kim
sskim@halla.ac.kr

한라대학교 HALLA UNIVERSITY

Contents

1 개인정보와 가명처리된 정보(법적정의)

1.1 개인정보보호법 제2조 제1호 : 개인정보의 정의

- "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(개인식별정보, (직접)식별자)

  나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. (개인식별가능정보, 간접식별자 혹은 준식별자) 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.

가명정보와 가명처리의 정의

다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보"라 한다)

- 제2조 제1호의 2(신설)

◦ "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

1.1 개인정보보호법 제2조 제1호 : 개인정보의 정의

- (기존) 개인정보
  - 가목 또는 나목 : 개인식별 정보 또는 개인식별 가능 정보
- (개정) 개인정보
  - 가목 또는 나목 + 가명정보

신용정보법 제2조(정의)

15. "가명처리"란 추가정보를 사용하지 아니하고는 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리(그 처리 결과가 다음 각 목의 어느 하나에 해당하는 경우로서 제40조의2제1항 및 제2항에 따라 그 추가정보를 분리하여 보관하는 등 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리한 경우를 포함한다)하는 것을 말한다.

가. 어떤 신용정보주체와 다른 신용정보주체가 구별되는 경우

나. 하나의 정보집합물(정보를 체계적으로 관리하거나 처리할 목적으로 일정한 규칙에 따라 구성되거나 배열된 둘 이상의 정보들을 말한다. 이하 같다)에서나 서로 다른 둘 이상의 정보집합물 간에서 어떤 신용정보주체에 관한 둘 이상의 정보가 연계되거나 연동되는 경우

다. 가목 및 나목과 유사한 경우로서 대통령령으로 정하는 경우

16. "가명정보"란 가명처리한 개인신용정보를 말한다.

1.2 가명처리의 대상, 방법 및 기준

- 가명처리의 대상
  - 가목 또는 나목 : 개인식별 정보 또는 개인식별 가능 정보
  - 개인정보보호법 제3절 가명정보처리에 관한 특례에 따라 제23조의 민감정보와 제24조의 고유식별정보 포함, 단 주민등록번호는 제24조의 2에 따라 제외, CI(Connecting Information)값은 전부가 아닌 일부를 사용하여 대체
- 가명처리 방법
  - 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등
- 가명처리의 기준
  - 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리
  - 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없도록 처리

1.3 가명정보의 처리에 관한 특례 [신설]

- 제28조의2(가명정보의 처리 등) ① 개인정보처리자는 **통계작성, 과학적 연구, 공익적 기록보존 등**을 위하여 **정보주체의 동의 없이** 가명정보를 처리할 수 있다.**(이용 목적 제한)** ② 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니된다.

- **기존** 제18조 2항(목적외 이용 등의 예외 항목) 4호 **(삭제)**
  - 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아 볼 수 없는 형태로 개인정보를 제공하는 경우

신용정보법 제32조(개인신용정보의 제공·활용에 대한 동의)

9의2. 통계작성, 연구, 공익적 기록보존 등을 위하여 가명정보를 제공하는 경우. 이 경우 **통계작성에는 시장조사 등 상업적 목적의 통계작성을 포함하며, 연구에는 산업적 연구를 포함한다.**

1.4 가명처리의 이용 목적 및 제3자 제공

- 가명처리의 대상
  - 가목 또는 나목 : 개인식별 정보 또는 개인식별 가능 정보
  - 개인정보보호법 제3절 가명정보처리에 관한 특례에 따라 제23조의 민감정보와 제24조의 고유식별정보 포함, 단 주민등록번호는 제24조의 2에 따라 제외 , CI(Connecting Information)값은 전부가 아닌 일부를 사용하여 대체
- 가명처리 방법
  - 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등
- 가명처리의 기준
  - 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리
  - 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없도록 처리
- 가명처리의 이용 목적
  - 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리
- 가명처리된 정보의 제3자 제공 가능

1.5 제28조의3(가명정보의 결합 제한)

- 제28조의3(가명정보의 결합 제한) ① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다. ② 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 개인정보처리자는 가명정보 또는 제58조의2에 해당하는 정보로 처리한 뒤 전문기관의 장의 승인을 받아야 한다. 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.
  - 제58조의2(적용제외) 이 법은 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보에는 적용하지 아니한다.

신용정보법 제2조(정의)

17. "익명처리"란 더 이상 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리하는 것을 말한다.

1.6 서로 다른 개인정보처리자 간의 가명정보의 결합

- 가명처리의 대상
  - 가목 또는 나목 : 개인식별 정보 또는 개인식별 가능 정보, 제23조의 민감정보, 제24조의 고유식별정보
- 가명처리 방법
  - 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등
- 가명처리의 기준
  - 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리
  - 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없도록 처리
- 가명처리의 이용 목적
  - 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리
- 가명처리된 정보의 제3자 제공 가능
- 서로 다른 개인정보처리자간의 가명정보 결합 가능
  - 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 목적으로 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행
  - 전문기관의 승인을 통해 가명정보 혹은 익명정보로 반출 가능

1.7 가명정보의 처리에 관한 특례 (신설)

- 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 대통령령이 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 위해 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다.
- 제28조의5(가명정보 처리 시 금지의무 등) ① 누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니된다. ② 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다.
- 제28조의6(가명정보 처리에 대한 과징금 부과 등) ① 보호위원회는 개인정보처리자가 제28조의5제1항을 위반하여 특정 개인을 알아보기 위한 목적으로 정보를 처리한 경우 전체 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 4억원 또는 자본금의 100분의 3 중 큰 금액 이하로 과징금을 부과할 수 있다. ② 과징금의 부과·징수 등에 필요한 사항은 제34조의2제3항부터 제5항까지의 규정을 준용한다.

2 가명처리 세부사항

2.1 가명처리의 대상(법적·기술적 관점)

- 개인정보보호법 제2조 1호 가목 또는 나목 : 개인식별 정보 또는 개인식별 가능 정보
  - 개인정보보호법 제3절 가명정보처리에 관한 특례에 따라 제23조의 민감정보와 제24조의 고유식별정보 포함, 단 주민등록번호는 제24조의 2에 따라 제외
- ISO/IEC 20889 : PEDD 용어와 기술분류 - (직접)식별자, 간접식별자(준식별자)
  - 데이터 주체의 식별자(또는 복수의 식별자)를 가명으로 대체하여 데이터 주체의 신원을 숨기는 비식별화 기술
  - 가명화는 모든 직접 식별자 및 잠재적으로 일부 추가적인, 또는 모든 잔여 식별 속성을 가명으로 대체하는 것을 포함함
- ISO 25237 보건의료 – 가명화
  - 가명화는 일반적으로 직접 식별자에 대해 사용되지만 결과 데이터 집합의 의도된 사용에 대한 장기적인 요구를 유지하면서 위험을 줄이기 위해 간접 식별자에 대해 사용될 수도 있다.
- EU ENISA, An overview on data pseudonymisation, 2018
  - 제4조 (1) GDPR에서 개인 정보의 정의에 따라, 즉 식별되거나 식별 가능한 사람과 관련된 정보는 실제로 가명화 된 데이터가 데이터 주체의 직접적인 또는 간접적 식별을 허용하지 않아야 함을 의미한다.(추가 정보의 이용이 없이). 따라서 GDPR에 따른 가명화는 '실제 인물 식별'의 보호를 넘어 데이터 주체와 관련된 간접 식별자의 보호를 포함한다.

2.2 가명처리의 수준(법적관점)

- **EU GDPR**
  - Article 4 (5) '가명처리'는 추가 정보(additional information)의 사용 없이는 개인정보가 더 이상 특정 정보주체에게 귀속되지 않는 방법으로 개인정보를 처리하는 것을 의미한다. 이 때 개인정보가 식별된 또는 식별가능한 정보주체 에게 귀속되지 않도록 그러한 추가 정보는 분리 보관되며 기술적 관리적 보호 조치의 적용을 받아야 한다는 점에 전제되어야 한다.
  - Article 5 (1) (b) 개인정보는 특정되고, 명시적이며, 적법한 목적으로 수집되어야 하며, 이러한 목적과 양립불가능한 방법으로 추가적으로 처리되어서는(further processed)* 아니된다. 제89조 제1항에 부합하는 공익을 위한 기록보존 목적, 과학적 또는 역사적 연구 목적 또는 통계 목적의 추가적인 처리는, 당초 목적과 양립불가능한 것으로 보지 않는다.
  - Article 89 (1) 공익을 위한 기록 보존 목적, 과학적 또는 역사적 연구 목적 또는 통계적 목적은 정보주체의 권리와 자유를 보호하기 위하여 본 규칙에 부합하는 적절한 보호조치의 대상이 되어야 한다. 이러한 조치에는, 이러한 목적들이 그러한 방법으로 달성될 수 있다면 가명처리를 포함할 수 있다. 이러한 목적이 정보주체의 개인식별을 허용하지 않거나 더 이상 허용하지 않는 추가적 처리에 의하여 달성될 수 있다면, 그러한 목적은 그러한 방법으로 달성되어야 한다.
  - * 추가적 처리 : 개인정보가 특정 목적으로 수집된 후 그와 다른 목적으로 처리되는 경우를 말함
  - (결론) EU GDPR에서의 가명처리는 단순히 기술적 관리적 보호조치의 일환임
    - 아울러 서로 다른 개인정보처리자간의 가명정보 결합에 대한 명시적 조항도 없음

2.2 가명처리의 수준(법적관점)

- **개인정보보호법**
  - 제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.
  - 제28조의7(적용범위) 가명정보는 제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지), 제21조(개인정보의 파기), 제27조(영업양도 등에 따른 개인정보의 이전 제한), 제34조(개인정보 유출 통지 등)제1항, 제35조(개인정보의 열람), 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처리 정지 등), 제39조(손해배상책임)의3, 제39조의4, 제39조의6부터 제39조의8까지의 규정을 적용하지 아니한다.
  - 따라서 EU의 GDPR에서 말하는 가명처리(명시적 배제 조항이 없음)보다 우리나라의 개인정보보호법이 더 높은 예외인정과 규제 완화를 부여
  - (결론) 우리나라의 경우는 EU GDPR과 목적부터 다름
    - EU GDPR : 가명처리는 개인정보의 단순 기술적 관리적 보호조치의 일환
    - 우리나라 개인정보보호법 : 가명처리는 단순 보호조치가 아닌 개인정보 안전한 활용이 목적
    - 따라서 보호조치의 수준은 EU GDPR보다 높을 것으로 전망됨

2.2 가명처리의 수준(기술적관점)

- EU ENISA, An overview on data pseudonymisatin, 2018
  - 특정 데이터 주체를 식별 할 수 있는 식별자의 가능성은 그것이 적용되는 특정 맥락(Context)과 매우 관련이 있으며, 이는 다른 맥락에서 실제로 동일한 식별자가 동일한 데이터 주체의 상이한 식별 수준을 제공 할 수 있음을 의미한다.
- EU ENISA, Pseudonymisation and best practices, 2019
  - Risk-based approach towards pseudonymization
  - 필요한 유틸리티 수준을 평가하고 관련 유틸리티 및 확장성 요구를 고려하면서 위험 기반 접근 방식을 채택해야함
  - 데이터 컨트롤러와 프로세서들은 이루고자 하는 유용성과 확장성 레벨 뿐만 아니라 데이터 이용 목적과 개인정보 처리에 대한 전반적인 컨텍스트를 고려해야함
- ISO/IEC 20889 : PEDD 용어와 기술분류
  - 가명으로 대체될 속성의 선택은 각 사용 사례별로 다르기 때문에, 조직의 목표 및 재식별화 위험성의 평가에 따라 실행해야 함

2.2 가명처리의 수준(기술적관점)

- ISO 25237 보건의료 – 가명화
  - 프라이버시 보호의 보장단계
    - 1단계 : 분명하게 식별되는 데이터 또는 쉽게 얻을 수 있는 간접 식별 데이터의 제거
    - 2단계 : 공격자가 외부 데이터를 사용할 때를 대비 - 이 단계에 대한 절차를 정의할 때 정적인 위험 분석이 검토되며, 그것은 다른 사용자에 의해 재식별의 약점이 있을 때를 대비한 것이다. 추가적으로 특정 데이터 집합을 식별하기 위해 가명화된 데이터와 외부 데이터를 결합하여 공격하는 존재에 대해서도 대비를 해야 함
    - 3단계 : 데이터의 특이치들(outliers)에 대한 대비
- (시사점) 처리 수준 정의시 고려사항
  - 개인정보 내 하나의 정보(직접식별자)로 개인을 식별할 수 있는 경우(위 1단계에 해당)
  - 개인정보 내 직접식별자를 가명처리 후 다른 정보(일부 또는 전부의 간접식별자 또는 외부 데이터*)와의 조합을 통해 개인을 식별할 수 있는 경우(위 1, 2단계에 해당)

    * (예) 제3자 제공시 제공받는자가 보유한 다른 정보
  - 직접식별자와 간접식별자를 처리한 후에도 특정 속성값 하나(특이치)만으로 개인을 식별할 수 있는 경우(위 3단계에 해당) : 예(희귀질환, 낙인성 정보 등)

2.3 가명처리 절차

- 1단계 : 가명처리 목적 검토(법적 부합성)
- 2단계 : 목적에 따른 가명처리 대상(최소화의 원칙) 선별, 데이터 정제
- 3단계 : 가명처리 대상에 따른 위험도 측정
  - 처리환경 즉, 맥락(Context)을 고려 : 내부 활용 또는 내부 제공, 내부 결합, 외부 제3자 제공에 따라 위험도가 다름
  - 이용기관 또는 제공받는 기관의 개인정보보호수준을 고려
- 4단계 : 위험도에 따른 처리 수준 정의
  - 3단계에서 측정한 위험도(상중하 등)에 따라 처리 수준 정의
- 5단계 : 가명처리
  - 4단계에서 정의한 처리수준에 따라 속성별 가명처리
- 6단계 : 적정성 검토
  - 5단계에서 처리한 처리 결과 데이터에 대한 적정성(4단계 처리 수준 정의에 따라 적절히 처리가 수행되었는지) 검토
- 7단계 : 사후관리
  - 추가정보에 대한 별도 분리 보관, 내부관리계획에 따라 기술적·관리적 보호조치 수행

2.4 가명처리 방법

- 법적 정의
  - 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리
  - 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없도록 처리
- 추가정보
  - 개인 데이터를 특정 데이터 주체로 귀속시키기 위한 정보로서 원본(가명처리 대상) 식별자와 가명처리된 가명정보와의 연관성을 나타내는 정보

<원본정보(예시)>

성명
김희선
권율
강수지
이순신
박은하
장동건
정우성
이황
오동구

<가명정보(예시)>

성명
최수지
권민준
강하늘
김라희
박민지
최재영
박상희
강윤희
육동희

<매핑테이블> 추가정보

원본성명	가명
김희선	최수지
권율	권민준
강수지	강하늘
이순신	김라희
박은하	박민지
장동건	최재영
정우성	박상희
이황	강윤희
오동구	육동희

2.4 가명처리의 방법

대체 기법	세부 기술
양방향 암호화	- 대칭키 암호화 - 공개키 암호화 - 키 삭제를 통한 결정적 암호화
일방향 암호화	- 키가없는 해시 암호화 - 키가 필요한 해시 암호화 SHA-2이상 - 솔트(Salt)를 추가한 해시 암호화
마스킹	- 부분 대체 - 스크램블링(Scrambling) 또는 셔플링(Shuffling) - 블러링(Data blurring)
기타	- 의사 난수 생성(Pseudo-Random Number Generator) - 카운터(Counter) - 토큰화(Tokenization)

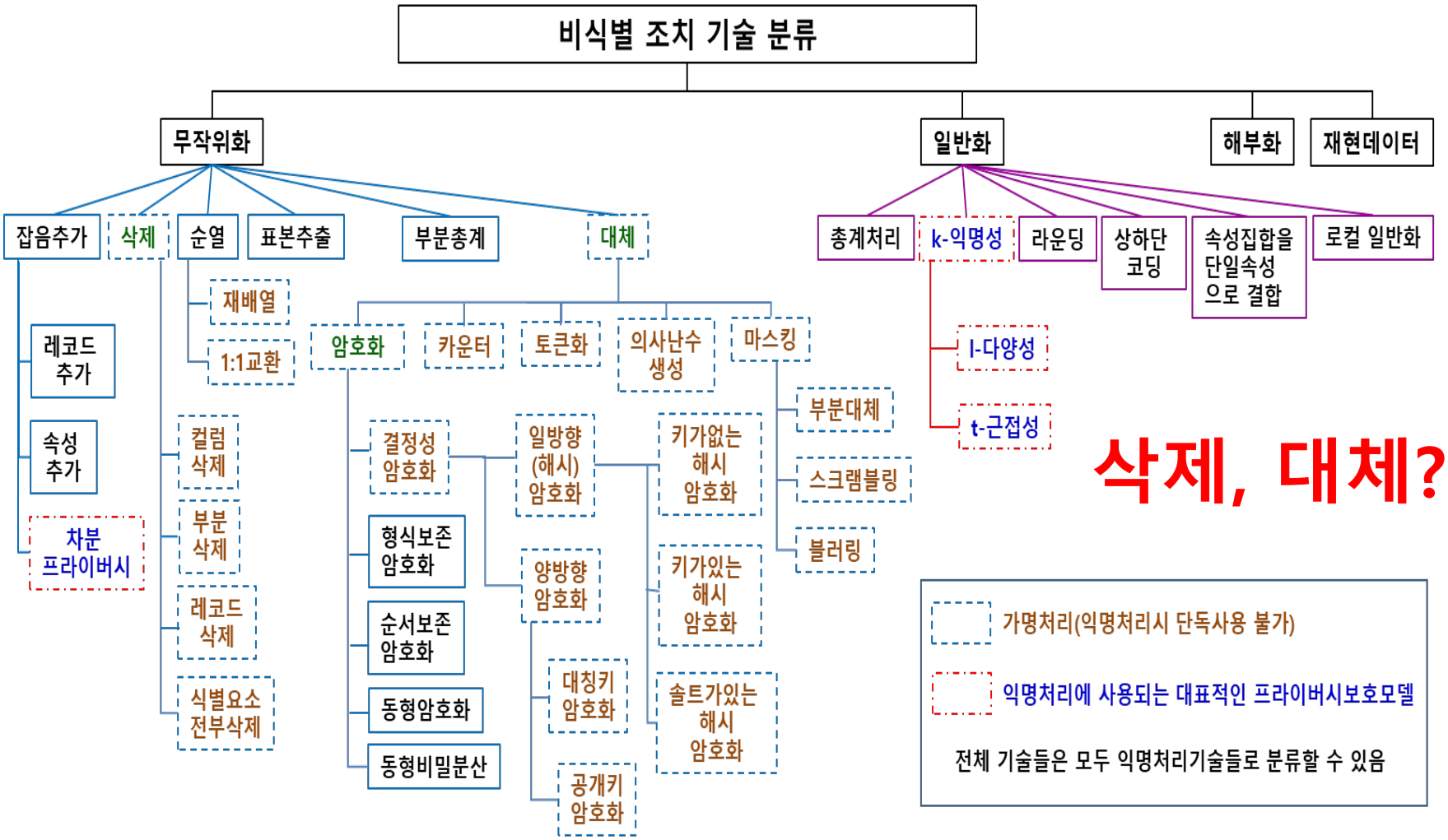
- EU ENISA, An overview on data pseudonymisatin, 2018
- EU ENISA, Pseudonymisation and best practices, 2019
- ISO/IEC 20889, 2018. 11

2.4.1 마스킹

- 부분대체 : 김순석 -> 김XX, 질병코드 F28 -> FXX, 나이 38세 -> 3X
- 스크램블링(문자 permutation, 단순한 형태의 대칭형 암호화로 간주될 수 있음)
  - 약한 가명, 비권장
  - 신용카드번호 예시
    - 4678 3412 5100 5239-> XXXX XXXX XXXX 5239 : 부분대체
    - 4678 3412 5100 5239-> 0831 6955 0734 4122 : 스크램블링
  - 그러나 제한 사항에도 불구하고 특정 상황에서 일정 수준의 보호를 제공하는 데 사용될 수 있음(예 : 마스킹 된 전화 번호는 청구 목적으로 구내에서 이루어진 전화 통화를 표시하는 데 사용될 수 있음).
- 블러링
  - 반올림이나 이미지 흐림(최근의 연구에 따르면 인공 신경망을 기반으로 한 이미지 인식 기술은 이러한 흐릿한 이미지에서 숨겨진 정보를 복구 할 수 있음)

[출처] ENISA(European Union Agency for Network and Information Security), Recommendations on shaping technology according to GDPR provisions, An overview on data pseudonymisatin, November 2018.

2.4 가명처리의 방법


비식별 조치 기술 분류
무작위화
일반화
해부화
재현데이터
잡음추가
삭제
순열
표본추출
부분총계
대체
총계처리
k-익명성
라운딩
상하단 코딩
속성집합을 단일속성으로 결합
로컬 일반화
l-다양성
t-근접성
레코드 추가
속성 추가
차분 프라이버시
재배열
1:1교환
컬럼 삭제
부분 삭제
레코드 삭제
식별요소 전부삭제
암호화
카운터
토큰화
의사난수 생성
마스킹
부분대체
스크램블링
블러링
결정성 암호화
일방향 (해시) 암호화
키가없는 해시 암호화
키가있는 해시 암호화
솔트가있는 해시 암호화
양방향 암호화
대칭키 암호화
공개키 암호화
형식보존 암호화
순서보존 암호화
동형암호화
동형비밀분산
삭제, 대체?
가명처리(익명처리시 단독사용 불가)
익명처리에 사용되는 대표적인 프라이버시보호모델
전체 기술들은 모두 익명처리기술들로 분류할 수 있음

2.5 가명처리시 기술적 고려사항

- 내외부 공격자 고려
  - 내부 개인정보 정보처리자나 TTP(전문기관)이 공격자가 될 수도 있음
  - 모든 시나리오에서 악의적으로 행동하고 일하는 행위자는 외부의 적으로 간주되어야함
- 기술적 공격에 대한 대비 필요
  - 무차별 대입 공격(Brute force attack)
    - 해당 가명에 대해 원본값을 찾을 때까지 모든 가능한 원본값들을 대입해 봄
  - 사전 공격(Dictionary Search)
    - 원본값에 해당하는 모든 가명에 대한 매핑테이블을 미리 계산하여 적용
    - Rainbow 테이블 또는 Hellman 테이블 등이 있음
  - 추측(Guesswork)
    - 공격자가 일부 배경지식(확률분포, 발생 빈도, 기타 부가정보 등)을 사용, 식별자의 통계적 특성을 이용, 공격

* EU ENISA(European Union Agency for Network and Information Security), Pseudonymisation and best practices, Non. 2019

2.6 가명처리 방법별 추가정보의 예시

가명화 기술의 종류			추가정보
삭제			-
대체	양방향 암호화	대칭키 암호화	대칭키, 암호 알고리즘
		공개키 암호화	공개키, 개인키, 암호 알고리즘
		키 삭제를 통한 결정적 암호화	결정적 암호화에 사용된 키, 암호 알고리즘
	일방향 암호화	키가없는 해시 암호화	해시 암호화 알고리즘(비권고)
		키가 필요한 해시 암호화	해시 암호화 키, 해시 암호화 알고리즘
		솔트(Salt)를 추가한 해시 암호화	솔트값, 해시 암호화 알고리즘
	마스킹	부분 대체	매핑테이블
		스크램블링(Scrambling) 또는 셔플링(Shuffling)	
		블러링(Data blurring)	
	의사 난수 생성(Pseudo-Random Number Generator)		의사난수생성 알고리즘, 매핑테이블, (필요시) 초기 Seed값
	카운터(Counter)		매핑테이블
	토큰화(Tokenization)		토큰생성 정보(암호화 등), 매핑테이블

2.7 특이치

- 특이치(이상치, Outlier)에 대한 추가 처리
  - 개인정보 내 개인식별정보나 개인식별가능정보 중 일부를 삭제하거나 일부 또는 전부를 대체하더라도 남아있는 정보(들)을 이용하여 의도치 않게 특이항목 내에서 특이치를 발견하여 공개적으로 쉽게 이용 가능한 정보(입수가능성 등을 고려)나 개인적 지식(Personal knowledge)* 을 이용하여 특정 개인을 식별할 수 있음
  - 예시) 주소 : 서울시 광진구, 직업 : 국회의원
  - 정치인(국회의원, 시장, 고위 공직자 등), 유명인(연예인, 스포프 선수 등), 공인, 셀렙 등
  - 직업이 소득 또는 재산 등 금융정보, 의료 민감정보, 희귀(질환)정보들과 함께 있는 경우
  - 부모가 유명인인 후손의 교육 데이터 즉, 교육 데이터에 부모가 유명 연예인이 있는 경우
  - 희귀(질환, 희귀 성씨))정보와 낙인성(다문화가정, HIV, AIDS, Corona virus 등) 정보
    - 낙인성 정보 : 외모와 관련(신체 기형), 소속집단(국적, 특이종교, 유색인종 등)
    - 희귀정보 : 수요에 비하여 공급이 상대적으로 부족한 경우의 정보(주로 희귀 질환)

* 영국 아일랜드 데이터보호위원회(The Data Protection Commission (DPC)), Guidance Note: Guidance on Anonymisation and Pseudonymisation, pp. 10, June 2019, https://www.dataprotection.ie/en/guidance-landing/anonymisation-and-pseudonymisation

2.7 특이치

- 국내 희귀 성씨

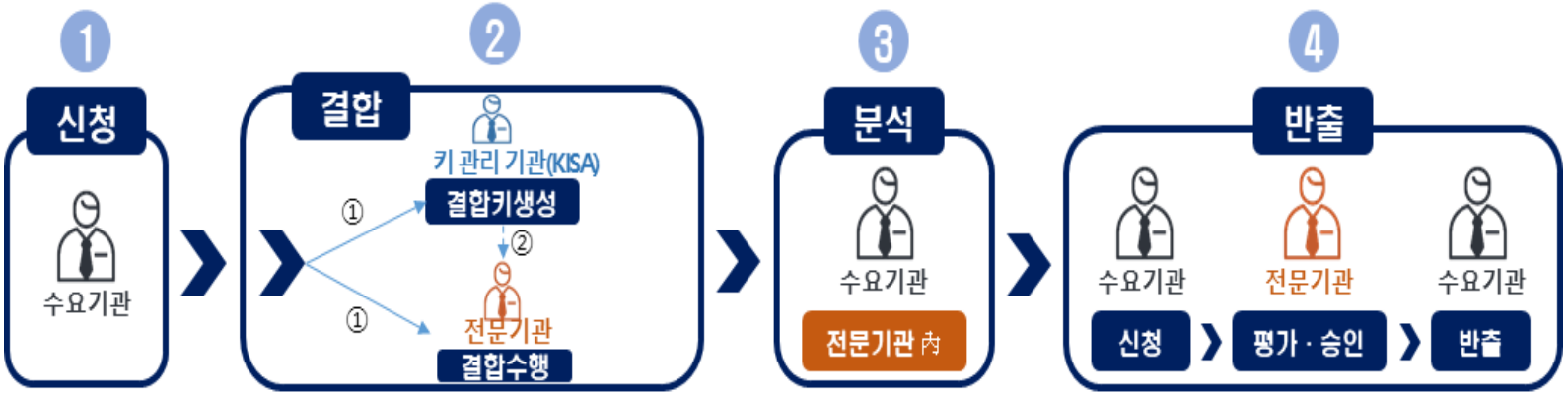
2.8 전문기관을 통한 가명정보 결합

- 개인정보보호법 시행령 주요사항
  - (전문기관) '특정 개인을 알아볼 수 없도록 보호위가 고시하는 절차와 방법'에 따라 가명정보를 결합하고, 이 과정에서 안전한 결합을 위한 지원 * 가능

* 한국인터넷진흥원 등이 결합에 필요한 연계정보를 생성하고 결합기관에 제공

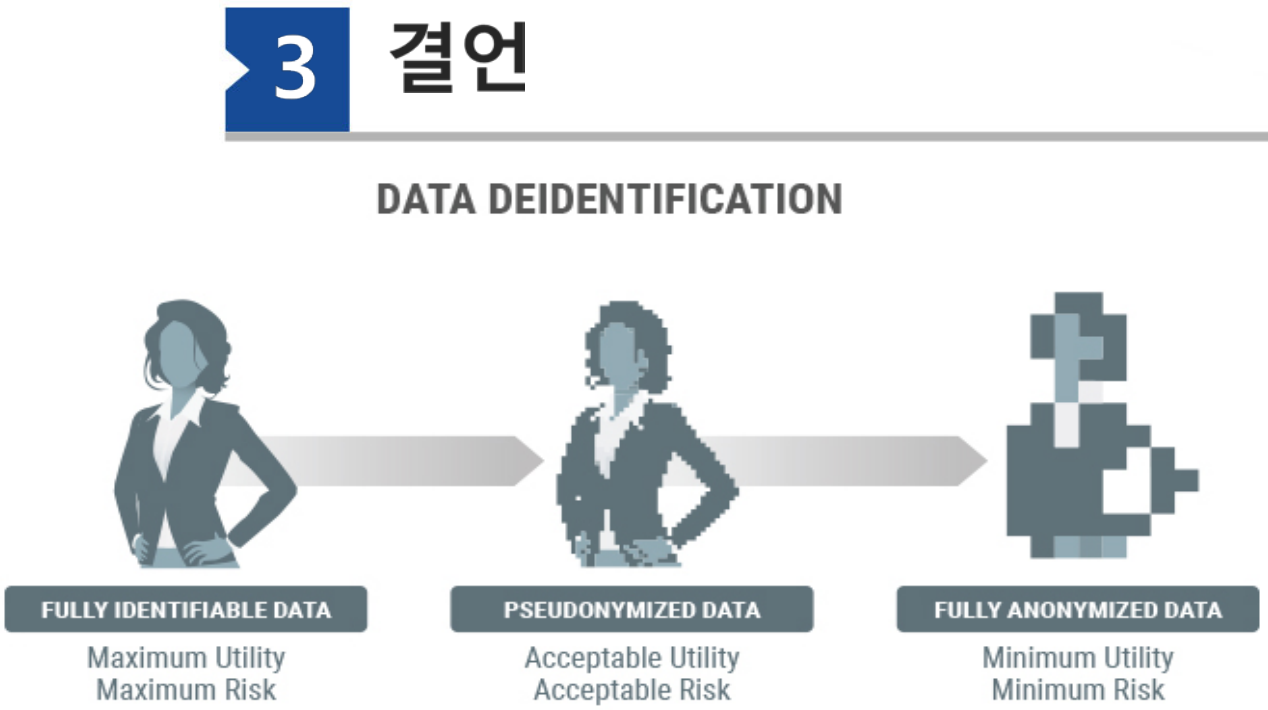
- (반출심사) 전문기관에 반출 적정성 심사 위원회(3명 이상)를 구성하여, 반출 여부와 적정한 반출 수준을 심사 *

* ▲반출된 정보를 제공받은 기관이 원래 보유한 정보와 반출된 정보를 결합하여 개인을 알아볼 가능성이 없는지, ▲반출정보의 처리 목적과 환경에 비추어 안전성 확보 조치계획이 적정한지, ▲데이터 성격에 따른 보유기간의 적정성 및 반출 목적 달성 후 파기 계획이 적정한지 등을 종합적으로 검토하여 심사



* 관계부처합동 데이터 3법 시행령 입법예고 주요사항, 3월 31일 보도자료

3 결언

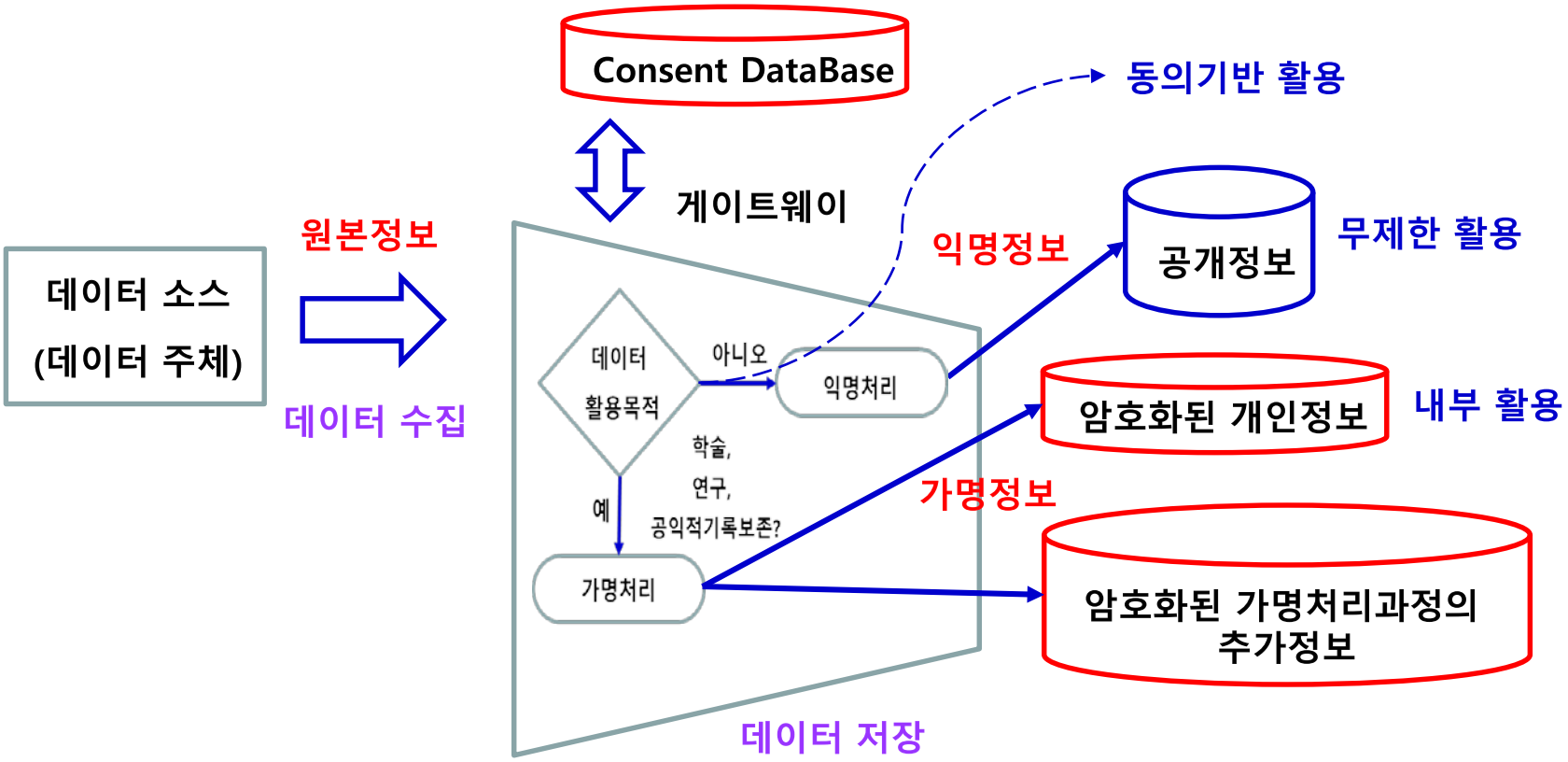


https://www.tokenex.com/blog/general-data-protection-regulation-pseudonymization-vs-anonymization

3.1 개인정보·가명정보의 범위, 대상, 방법 및 기준

<table>
<tr><th></th><th colspan="2">개인정보보보호법</th><th colspan="2">신용정보법</th></tr>
<tr><td rowspan="5">개인정보의 범위</td><td colspan="4">개인식별정보</td></tr>
<tr><td colspan="4">개인식별가능정보</td></tr>
<tr><td colspan="2" rowspan="3">가명처리된 정보</td><td rowspan="3">가명처리된 정보</td><td>신용정보주체가 구별되는 경우</td></tr>
<tr><td>둘이상의 정보가 연계되거나 연동되는 경우</td></tr>
<tr><td>대통령령으로 정하는 경우</td></tr>
<tr><td>가명처리의 대상</td><td colspan="4">개인식별정보 또는 개인식별가능정보</td></tr>
<tr><td rowspan="2">대상별 가명처리 방법</td><td colspan="4">개인식별정보 : 삭제 또는 대체</td></tr>
<tr><td colspan="4">개인식별가능정보 : (Context와 Risk 측정에 기반 상황에 따라) 일부 또는 전부를 대체, 추가처리(특이치(Outlier))</td></tr>
<tr><td>가명처리 기준</td><td colspan="2">특정 개인에 대한 식별가능성이 없어야함</td><td colspan="2">신용정보주체가 구별되고 둘이상의 정보가 연계되거나 연동되어도 특정 신용정보 주체에 대한 식별가능성이 없어야함</td></tr>
<tr><td>익명처리 기준</td><td colspan="2">시간・비용・기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없도록 처리
※ 법에서 익명처리란 용어를 명시적으로 사용하지 않음</td><td colspan="2">더 이상 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리</td></tr>
</table>

3.2 기업 내 가명 데이터 관리 프로세스의 예



Q & A