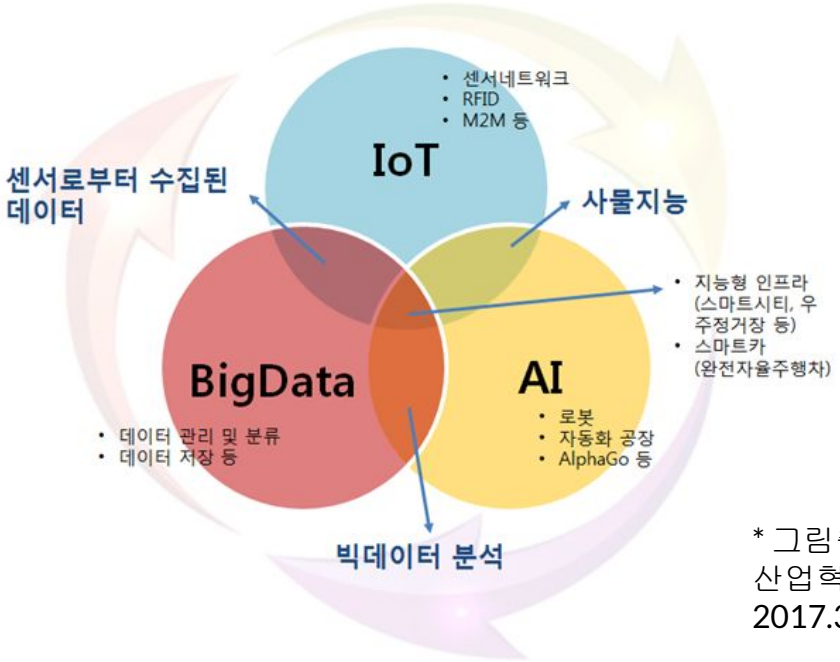
건강정보 보호 및 보건의료 연구를 위한

개인정보보호법 개정 방향

오병일 (진보네트워크센터 대표)

신기술과 개인정보

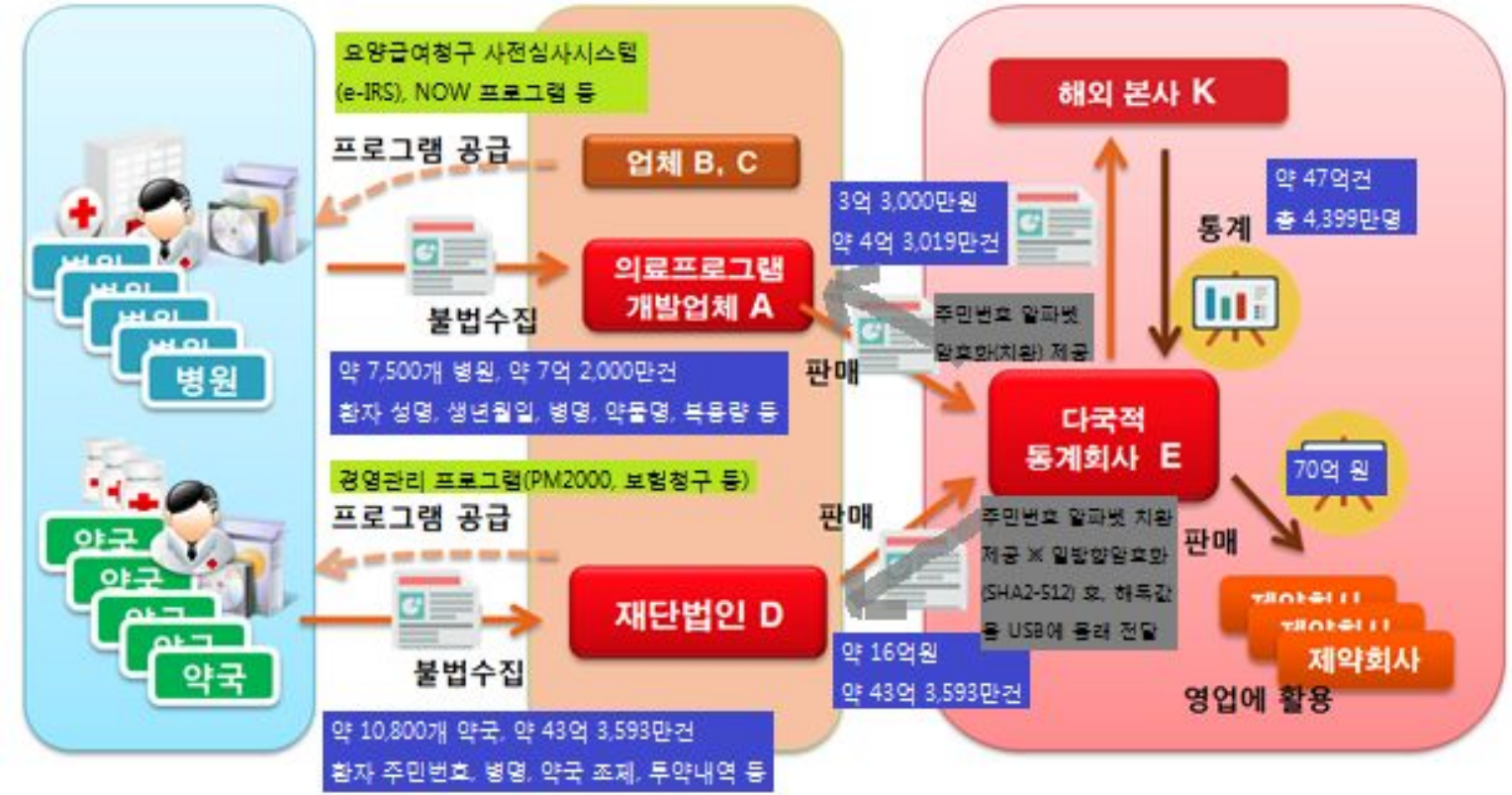


* 그림출처 : IT DAILY, [전문가 강좌] 4차 산업혁명과 지능정보기술의 미래방향 (3), 2017.3.2

개인정보 침해 위협의 증가

- 정보주체도 모르는 개인정보 수집 : 인터넷 이용기록, 교통카드, 시청기록, 결제기록 등
- SNS 등을 통한 적극적인 개인정보의 공개
- 사물인터넷(IoT)과 개인정보 수집의 획기적인 증가
- 서로 다른 개인정보 처리자의 연계
  - 앱 개발자 - 플랫폼 운영자 - 빅데이터 분석가 - 제휴업체 - 유통업자
- 빅데이터 분석 등 개인정보의 목적 외 활용 요구 증가
- IoT 등 보안위협
- 개인정보의 국제이전

IMS헬스 사건 - 처방전 매매



빅데이터와 개인정보 이슈 주요 경과

- 2016.6 : 관계부처합동, <개인정보 비식별조치 가이드라인> 발표
  - 2016.8~2017.9, 26차례에 걸쳐 총 347,522,005건의 민간 기업의 데이터 결합
- 2017.11.9 : 시민단체, 비식별화 전문기관 및 20개 기업 고발
- 2018.2. / 2018.4 : 대통령산하 제4차산업혁명위원회, 규제.제도혁신 해커톤 개최
- 2018.8.31 : 문재인 대통령, 데이터 경제 활성화 규제혁신 방안 발표
- 2018.11.15 : 정부, 개인정보보호법 개정안 발의(인재근 의원안)
  - 정보통신망법 및 신용정보법 개정안도 발의됨. (빅데이터 3법)

규제제도혁신 해커톤

- 2차 해커톤 (2018.2)
  - 개념체계 정비 : 개인정보, 가명정보, 익명정보
  - 익명정보는 법에 명시하지 않고, EU GDPR 전문(26)을 참조하여‘개인정보’의 개념을 보완.
  - 가명정보에 대한 법적 근거 마련 필요
- 3차 해커톤 (2018.4)
  - 가명정보는① 공익을위한 기록보존의 목적, ② [학술연구/ 학술및연구] 목적, ③ 통계목적을 위하여 당초 수집목적외의 용도로 이용하거나 이를 제3자에게 제공할수있다고 합의. [학술 연구 / 학술 및 연구] 목적에는 산업적 연구 목적이 포함될 수 있고, 통계 목적에는 상업적 목적이 포함될 수 있다는 점에 동의
  - 최초 수집목적과 양립되는 추가적인 개인정보 처리
  - 개인정보의 결합과 관련해서는 미합의

쟁점[1] 개인정보의 개념

- "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다(개인정보보호법 제2조).
- 정부의 해석
  - (‘알아볼 수 있는’의 의미)는 해당 정보를 ‘처리하는 자’의 입장에서 합리적으로 활용될 가능성이 있는 수단을 고려하여 개인을 알아볼 수 있다면 개인정보에 해당
  - (‘쉽게 결합하여’의 의미)는 결합 대상이 될 정보의 ‘입수 가능성’이 있어야 하고 ‘결합가능성’이 높아야 함을 의미

개인정보의 개념 : 판례

- 대전지법 논산지원(2013고단17 판결) 2013.8.9 선고
  - 휴대전화번호 4자리도 개인정보
  - 휴대전화번호 뒷자리 4자만으로도 그 전화번호 사용자가 누구인지를 식별할 수 있는 경우가 있고, 특히 그 전화번호 사용자와 일정한 인적 관계를 맺어온 사람이라면 더더욱 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.
- 서울중앙지방법원(2010고단5343 판결) 2011. 2. 23. 선고
  - IMEI 및 USIM 정보도 개인정보
  - 기계적인 정보라도 특정 개인에게 부여됐음이 객관적으로 명백하고, 이러한 정보를 통해 개인이 식별될 가능성이 크다면 이를 개인정보로 봐야 한다고 판단

개인정보 개념 : 인재근 의원안

- 제2조(정의)
  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)
- 제58조의2(적용제외) 이 법은 시간·비용·기술 등 개인정보처리자가 활용할 수 있는 모든 수단을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보에는 적용하지 아니한다.

개인정보 개념 : GDPR

- Article 4 Definition
  (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- Recital 26: To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the mount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

쟁점[2] 목적 외 활용의 범위와 요건

- 빅데이터 분석 등 상업적 연구 목적의 개인정보 활용 및 제공에 대한 기업의 요구
- 현행 개인정보보호법 제18조
  - 제18조(개인정보의 목적 외 이용·제공 제한)
    ② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

    4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우

과학적 연구의 범위 :인재근의원안

- 제2조 8. “과학적 연구”란 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 말한다.
- 정부안 제안이유 : “새로운 기술.제품.서비스의 개발 등 산업적 목적을 포함하는 과학적 연구...”
- 제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.
  ② 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함하여서는 아니 된다.

과학적 연구의 범위 : 유럽 GDPR

- 공익적인 기록 보존, 과학 및 역사 연구 또는 통계 목적의 개인정보 처리는 원래의 수집 목적과 양립되는 것으로 인정 (제5조)
- GDPR recital 159
  ...the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area.

과학적 연구의 범위 : 유럽 GDPR

- TFEU 179(1) : 연구자, 과학적(학술적) 지식 및 기술이 자유롭게 유통되는 유럽 연구 영역의 달성에 의해 과학적, 기술적 기반의 강화를 목적으로 하고 있음. 즉, 과학적(학술) 연구는 기업 내부적인 목적이 아니라, 해당 연구 영역에서 자유롭게 유통될 수 있는 지식 의미.

과학적 연구의 범위 : 유럽 국가들

- 영국 개인정보감독기구 ICO
  - "It does not apply to the processing of personal data for commercial research purposes such as market research or customer satisfaction surveys."
- 슬로바키아
  - 법률에서 과학적 연구의 개념과 어떤 기관이 과학적 연구를 수행하는 기관이 되기위한 특정 조건을 규정함.
    (연구 개발을 위한 국가지원조직에 대한 법 Act No. 172/2015 Coll. 2조 1-3호 및 정부와 중앙 행정 기관의 활동 조직에 대한 개정법 no. 575/2001 Coll.)
  - 연구 : 사회의 필요와 지식 발전의 이익을 위해 과학 및 기술 분야에서 수행되는 체계적이고 창의적인 활동.
- 크로아티아
  - 과학적 연구는 윤리 원칙과 기준에 대한 국내 및 유럽 법률 조항에 따라 수행해야 함.

[쟁점 3] 안전조치 및 권리 제한

- 인재근 의원안
  - 제28조의4(가명정보에 대한 안전조치의무 등)
    - 1항. 안전성 확보에 필요한 기술적.관리적 및 물리적 조치
    - 2항. 관련 기록의 작성 보관
  - 제28조의7(적용범위) ① 가명정보는 제20조, 제21조, 제27조, 제34조제1항, 제35조부터 제37조까지, 제39조의8을 적용하지 아니한다.
    ② 제2조제1호가목 및 나목 정보의 가명처리에 관하여는 제15조부터 제18조까지, 제39조의3을 적용하지 아니한다.
    - 가명정보에 대해서는 수집출처 등을 고지받을 권리(20조), 개인정보의 파기(21조), 영업양도 등에 따른 개인정보의 이전 제한(27조), 유출 통지(34조 제1항), 개인정보의 열람(35조), 정정, 삭제(36조), 처리정지(37조) 등 권리제한
    - 가명처리에 대해서는 정보주체의 동의(15조, 17조), 최소수집원칙(16조), 목적제한원칙(18조) 등 권리 제한

처리의 적법성 : 유럽 GDPR

- 제5조(개인정보처리원칙)
  - 1항(b) 목적제한의 원칙 규정. 다만, 공익적인 기록 보존, 과학 및 역사 연구 또는 통계 목적의 개인정보 연계·결합은 원래의 수집 목적과 양립되는 것으로 인정
- 제6조(처리의 적법성)
  - 1항. 모든 개인정보처리자는 다음 중 하나의 요건을 갖추어야 함. (a) 동의 (b) 계약수행 (c) 법적 의무 준수 (d) 정보주체 및 제3자의 중대한 이익에 필요한 경우 (e) 공익목적의 업무수행 혹은 공식적 권한의 수행 (f) 개인정보처리자 혹은 제3자의 정당한 이익 (단, 정보주체의 기본적 권리를 침해하지 않아야 함)
  - 애초 수집 목적과의 양립가능성 판단시 고려사항 : (a) 애초 수집 목적과의 연관성 (b) 개인정보 수집 맥락 (c) 개인정보의 성격 (d) 추가 처리의 잠재적 영향 (e) (암호화나 가명처리를 포함한) 적절한 안전조치 여부
- (가명처리된) 개인정보를 제3자에게 제공할 경우, 제공받는 개인정보처리자도 제6조의 요건을 갖추어야 함.

안전조치 및 권리 제한 : 유럽 GDPR

- 공익을 위한 자료 보관 목적, 과학 또는 역사 연구 목적이나 통계 목적을 위한 처리와 관련한 보호장치 및 적용 완화 (제89조)
  - 적절한 보호장치가 적용되어야 함. 그러한 보호장치는 특히 정보 최소화 원칙에 대한 존중을 보장하기 위한 기술적, 조직적 조치가 갖추어지도록 보장해야 함. 그러한 조치에는, 그러한 목적이 해당 방식으로 충족될 수 있는 경우, **가명화가 포함**될 수 있음. 정보 주체 식별을 허용하지 않거나 더 이상 허용하지 않는 추가 처리를 통해 그러한 목적이 충족될 수 있는 경우, 그러한 목적을 해당 방식으로 충족해야 함.
  - 정보주체의 열람권, 정정권, 처리제한권, 거부권 등을 제한할 수 있으나, 이는 그러한 권리를 보장하면 특정 목적의 달성을 심각하게 침해하거나, 그러한 권리를 제한이 목적달성에 필요한 경우에 한정

정보주체에의 고지

- 유럽 GDPR
  - 과학적 연구 및 통계 목적일 경우에도 개인정보 처리자가 정보주체에게 개인정보 처리에 관한 정보를 제공할 의미를 배제하지 않음.(GDPR 13조, 14조)
- 인재근의원안
  - 개인정보보호법 15조, 17조 등을 배제하여, 가명처리 및 가명정보에 대해 정보주체의 알 권리를 침해함.

데이터최소화의 원칙

- 유럽 GDPR
  - 데이터 최소화의 원칙 보장
  - 익명처리가 가능할 경우 가명처리가 아닌 익명처리 적용
- 인재근의원안
  - 과학적 연구 및 통계 목적으로 단지 '가명정보'를 처리할 수 있도록 하고 있음.

정보주체의 권리 제한

- 유럽 GDPR
  - 정보주체의 권리를 보장할 경우 특정 목적의 달성을 심각하게 침해하거나, 그러한 권리를 제한이 목적달성에 필요한 경우에만 제한 가능.
- 인재근의원안
  - 가명처리 및 가명정보에 대해 정보주체의 권리를 포괄적으로 제한

안전조치

- 유럽 GDPR
  - 위험성에 비례하는 안전조치 의무 부과
  - 가명처리는 안전조치의 하나가 될 수 있음.
- 인재근의원안
  - 가명정보에 대해서는 목적 외 활용 일괄 허용
  - 안전성 확보에 필요한 기술적.관리적 및 물리적 조치
  - 관련 기록 작성 보관

안전조치

- 룩셈부르크 : 처리의 성격, 범위, 맥락, 목적과 위험성 등을 고려하여 다음과 같은 추가적인 적절한 조치를 취해야 함 (룩셈부르크 개보법 65조)
  - 개인정보보호 담당관의 지정
  - 개인정보영향평가 수행
  - 익명화/가명화 조치, 혹은 과학적 연구 등을 목적으로 수집된 데이터가 정보주체와 관련된 결정에 사용되지 못하도록 보장하는 운영 분리 조치
  - 익명화/가명화를 위해, 처리자로부터 독립적인, 신뢰할 수 있는 제3자의 활용.
  - 전송 및 저장 데이터의 암호화 및 최신 기술을 이용한 키 관리
  - 정보주체의 사생활 보호 강화를 위한 기술 사용
  - 처리자 내부의 개인정보 접근 제한 조치
  - 누가, 언제, 왜 개인정보를 처리했는지에 대한 로그 파일
  - 개인정보 처리 및 직업적 기밀성에 대해 관련 직원 교육 증진
  - 독립적 감사를 통한, 기술적, 관리적 조치의 효과성에 대한 정기적인 평가
  - 사전적인 데이터 관리 계획 수립
  - GDPR 40조에 따른 특정 분야의 행동 강령 채택
  - 각 과학적, 역사적 연구 및 통계 프로젝트에 대해, 개인정보 처리자는 앞서 언급된 조치를 배제한 경우 이를 문서화하고 정당화해야 한다.

[쟁점 4] 정보집합물의 결합

- 인재근 의원안
  - 제28조의3(정보집합물의 결합) ① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 개인정보처리자간 정보집합물의 결합은 대통령령으로 정하는 기준에 따라 보안시설을 갖춘 전문기관이 수행한다.
    ② 결합을 수행한 기관 외부로 결합된 정보집합물을 반출하려는 개인정보처리자는 제2조제1호다목 또는 제58조의2에 해당하는 정보로 처리한 뒤 전문기관의 장의 승인을 받아야 한다.
  - 가명정보를 원 개인정보처리자에게 반출 허용
- GDPR에는 데이터 결합에 대한 별도 규정 없음.
  - 개인정보처리자는 각각 적법한 법적 근거를 가져야 함.
  - 데이터 보유기관, 연계기관, 연구자 사이의 엄격한 분리 원칙 적용

[쟁점 5] 개인정보 감독기구

- 완전히 독립적인 감독기구의 설치는 “개인정보의 처리와 관련하여 개인을 보호하기 위한 필수적인 구성요소” (유럽사법재판소, 2010)
- 현행 개인정보 보호체계의 문제
  - 법제의 분산 : 개인정보보호법, 정보통신망법, 신용정보법 …
  - 감독기구의 분산 : 행정안전부, 개인정보보호위원회, 방송통신위원회, 금융위원회
  - 감독기구의 독립성 부족
    - 행정안전부는 개인정보처리자이자 감독기구
    - 개인정보보호위원회는 인사 및 예산권, 집행권한 부재
  - 감독기구 분산으로 인한 혼란
    - 자의적인 규제대상 분할, 중복규제 혹은 규제의 공백, 이용자 혼란
  - 통일적인 개인정보 보호체계 수립에 장애
  - 감독기구의 전문성, 규제의 효율성 저해

보호체계 및 감독기구 : 인재근의원안

- 정보통신망법을 개인정보보호법으로 통합
- 행정안전부, 방통위의 감독권한을 개인정보보호위원회로 이관
- 신용정보법 및 금융위의 감독권한은 존속
- 개인정보보호위원회를 중앙행정기관으로 격상
- 개인정보보호위원회의 독립성 한계
  - 제7조(개인정보보호위원회) ① 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리 소속으로 개인정보 보호위원회(이하 “보호위원회”라 한다)를 둔다.
    ② 보호위원회는 「정부조직법」 제2조에 따른 중앙행정기관으로 본다. 다만, 다음 각 호의 사항에 대하여는 「정부조직법」 제18조를 적용하지 아니한다.
    1. 제7조의8제1항에서 정하는 소관사무 중 제3호 및 제4호의 사무
    2. 보호위원회의 심의·의결 사항 중 제1호에 해당하는 사항

개인정보보호법 정부안의 문제점

- (가명처리된) 개인정보의 폭넓은 상업적 활용, 제공, 결합 허용.
  - 통신, 금융, 의료 등 대기업 사이에 고객정보의 무한 공유 위험
- 개인정보 보호를 위한 안전장치 부재
  - 개인정보 감독기구의 독립성 미흡
  - 개인정보 영향평가 적용 제한
  - 프로파일링 권리 보장 및 규제 부재
  - 개인정보중심설계(Privacy by Design) 및 기본설정(Privacy by Default) 부재

개인정보보호법 개정 방향 제안

- 개인정보 정의 : 제3자에 의해서 식별 가능한 경우에도 개인정보로 규정
- 수집 목적 외 활용 범위는 '학술 연구'로 제한.
- 수집 목적 외 활용 시 안전조치 규정
  - 가명처리에 대해서도 정보주체에게 정보 제공
  - 데이터 최소화의 원칙 적용
  - 연구 및 통계 목적 달성시 개인정보 폐기
  - 예외적인 경우에만 정보주체의 권리 제한
  - 위험성에 비례하는 안전조치 의무화
- 개인정보 감독기구의 독립성과 권한 보장
- 개인정보 영향평가, Privacy by Design 등 처리자의 책임성 강화
- 프로파일링 권리 등 정보주체의 권리 강화

개인 건강정보와 연구

- 개인 건강정보에 대해서는 보다 엄격한 규율.
- 생체인식정보를 민감정보(제23조)에 포함.
- 보건의료 관련 법제에서 보건의료 데이터(개인 건강정보)의 안전한 활용을 위한 구체적인 거버넌스 규정
  - 사례 : 아일랜드, 건강 연구(health research)를 위한 적절하고 구체적인 안전조치 규정 (Health Research Regulation 2018 : Data Protection Act 2018 (Section 36(2)) : 아일랜드 개인정보보호법 Section 36 2항에 의해 만들어진, 건강 연구에 대한 추가 규정
    - 연구 목적 달성을 위해 필요한 개인정보에 한정
    - 해당 개인에게 피해를 야기하지 않아야 함
    - 적절한 거버넌스 구조를 갖춰야 함.
    - 연구 관리 및 수행과 관련된 절차 규정
    - 적절한 투명성 조치 : 웹사이트 혹은 공공장소에 공지, 개인에 대한 고지 등
    - 명백한 동의 (explicit consent)

해외 연구목적 제공 사례 : 뉴질랜드 통계청

연구자 프로젝트 보안 데이터 연구결과물