이용자 이익 보호를 위한 마이데이터

방 효 창 (경실련 정보통신위원장)

들어가기

- **개인정보보호법**
  - 제1조(목적) 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다. - 개인정보보호법? 사생활비밀보호법?

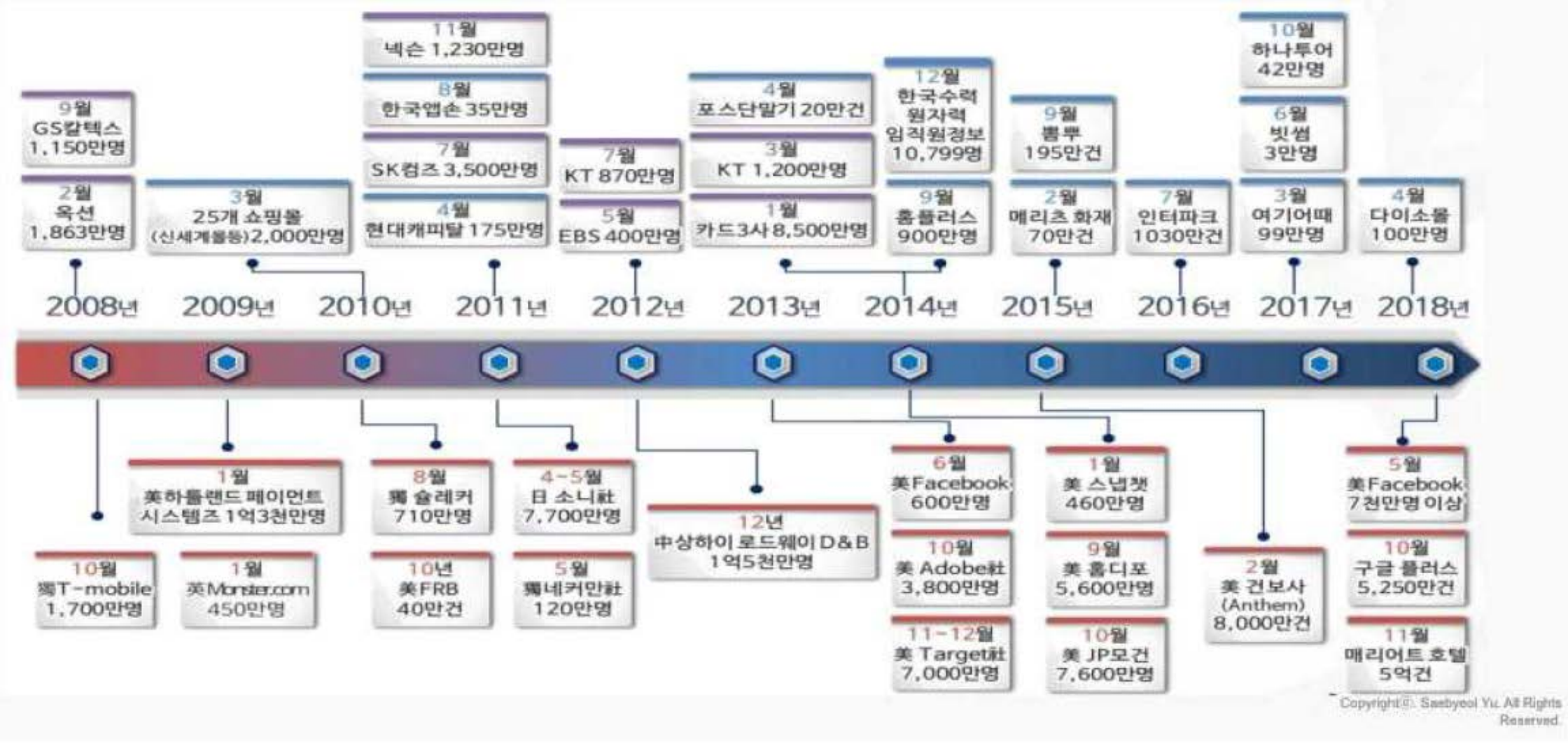
  - EU GDPR, 제1조(목적) ① 본 규칙은 개인데이터의 처리와 관련하여 자연인을 보호하기 위한 준칙과 개인데이터의 자유로운 이동을 위한 준칙을 정한다. ② 본 규칙은 자연인의 기본적 권리와 자유, 그리고 특히 개인데이터보호권을 보장한다. ③ 유럽연합 역내 개인데이터의 자유로운 이동은 개인데이터의 처리와 관련하여 자연인을 보호한다는 이유로 제한되거나 금지되어서는 안 된다.

  - 일본 개인정보보호법, 제1조(목적) 이 법률은 ---(중략)--- 개인정보를 취급하는 사업자가 준수하여야 할 의무 등을 규정함으로써 개인정보의 적정하고 효과적인 활용이 새로운 산업의 창출 및 활력 잇는 경제사회와 풍요로운 국민생활의 실현에 이바지하는 것이라는 점 외에 개인정보의 유용성을 고려하면서, 개인의 권리 이익을 보호하는 것을 목적으로 한다.

  - 국제프라이버시전문가협회(International Association of Privacy Professionals) – 한국은 세계에서 가장 엄격한 프라이버시보호법(the world's strictest privacy laws)을 가지고 있다. – Paul Sutton, Data Protection in South Korea: Why You Need to Pay Attention, Aug. 15, 2018. (?)

개인정보 유출 사고

출처 : 2019년 개인정보 실태점검 이슈와 계획 KISA



개인정보 유출 판결 사례

출처 : 한국개인정보법제연구회 김일영 변호사 2019 G-PRIVACY 컨퍼런스

	발생 시기	발생 원인	피해 규모(건)	적용 법률	민사 판결(원고 기준)			판결 주요 내용
					1심	2심	3심	
A사 오픈마켓	2008. 1	해킹	1,800만	정	×	×	×	고시 내 기술적 보호조치시 주의의무 위반 아니다(대법)
B 정유사	2008. 7.	수탁사 직원	1,100만	정	×	×	×	유출되어도 판매·유통되지 않으면 손해배상 의무 없다(대법)
C 포털 커뮤니티	2011. 7.	해킹	3,500만	정	○/×	○/×	×	고시 규정 없어도 기대가능한 보호조치 해야 한다(대법)
D 통신사 1차	2012. 7.	해킹	870만	정	○/×	○/×	×	개인정보처리시스템에 어플리케이션 포함(1,2심)
D 통신사 2차	2014. 2.	해킹	1,170만	정	○/×	×	-	개인정보처리시스템을 DB에 한정(1,2심)
카드3사	2010. 4 ~ 2013.12.	수탁사 직원	1억 400만	정/개	○(R사 2차×)	○(R사 2차×)	G사 : 10만	변환되지 않은 개인정보 제공, 수탁사 관리 미흡 위법(대법), 유출 후 유통되지 않아 손해배상 없음(R카드2차)
국내 마트 E 사	2014. 6.	내부원인	2,400만	개	○ 5/20만	-	-	대표이사, 임직원 형사 처벌(확정)
처방 정보 수집 및 판매	2014. 6.	내부원인	43억	개	×	-	-	-
해외 포털 사이트 F사	2014. 2.	내부원인	-	국제사법/정	일부 ○	-	-	글로벌기업에게 정보통신망법상 개인정보 제3자 제공 내역을 정보주체에게 제공할 의무 인정(1,2심)

이용자 관점에서의 데이터 3법

◆ 데이터 3법이 가져올 파장

- 금융, 의료, 통신 등 개인정보의 빅데이터화 추진
- 공공기관이 보유한 공공데이터의 개방(가명정보 처리)
- 개인정보보호위원회의 위상(독립성, 권한, 예산)? 금융위 신용정보? 개인의료정보?
- EU GDPR 적정성 평가?
- 규제 완화? 보호?
- 승자 독식 사회

개인정보보호법

◆ 개인정보보호법 개정(안)

- 개인정보의 범위
  - 개인정보 범위 축소 : 성명, 주민번호, 영상, 그리고 쉽게 결합하여 특정할 수 있는 정보
  - **(안) 개인정보처리자가** 활용할 수 있는 - EU **개인정보처리자**나 **다른 사람**에 의해 활용할 수 있는
- 가명처리된 개인정보의 상업적 목적 이용
  - 가명처리에서의 통계작성, "과학적 연구", 공익적 기록보존 - 개인정보처리자의 정당한 이익이 정보주체의 기본권 침해보다 클 경우에 한정
- 개인정보보호 감독기구의 독립성 및 예산
  - 국무총리 소속 개인정보보호위원회(제7조 2항만 독립), 정부의 지휘·감독 가능. 금융위, 보건복지부 권한 유지 : EU GDPR - 정부로부터 분리(독립)
- 개인정보 주체 권리 및 개인정보처리자의 책임성
  - 프로파일링에 대한 영향 평가, 개인정보 자기결정권(정보주체의 권리) 등 부재
  - 개인정보처리자의 강한 책임성 부재

신용정보법

◆ 신용정보법 개정(안)

- 개인정보보호법과의 중복, 혼란
  - 개인정보보호법제 일원화 정책에 역행 : 유사, 중복 조항 포함 – 정의, 가명처리/가명조치, 과학적연구/연구
  - 개인정보보호책임자 / 신용정보관리·보호인
- 가명 처리된 개인신용정보의 상업적 목적 판매
  - 가명처리에서의 통계작성, 연구, 공익적 기록보존 - 통계작성에는 상업적 목적의 통계 작성을 포함하며, 연구에는 산업적 연구를 포함한다.
- 익명 조치에 대한 책임성 부재
- 동의 없는 SNS 정보(공개된 개인정보) 수집(신용평가)
- 공공기관 보유 개인정보 공유 확대
  - 기존 : 공공기관 정보공개법, 개인정보보호법, 국민건강보험법, 국민연금법, 한국전력공사법, 주민등록법
  - 추가 : 국세기본법, 지방세기본법, 고용보험법, 산업재해보상보험법 등

신용정보법

◆ 신용정보법 개정(안)

- 자동화평가(프로파일링)에 따른 정보주체의 권리 보장

- 개인정보 이동권 – 제33조의2(개인신용정보의 전송 요구)
  - EU GDPR에서의 개인정보 이동권은 정보 독점을 방지하기 위해 정보주체의 권리를 강화
  - 개인정보보호법에서 개인정보 이동권을 적극 도입하여야 함.

- 본인신용정보관리법(일명 마이데이터 사업)
  - 정보주체의 권리를 대리
  - 사전동의(informed consent), 개인정보 처리의 투명화, 정보주체의 열람권

개인정보자기결정권

◆ 정보주체의 개인정보자기결정권

- 개인정보자기결정권
  - 개인정보자기결정권은 정보처리자가 행하는 개인정보처리의 전 과정을 '직접적으로 결정하거나 통제하는 권리 ' 가 아니다. 개인정보처리의 결정권은 개인정보를 처리하는 자에게 있다. EU GDPR은 개인정보처리자의 의미를 "단독 혹은 공동으로 개인 데이터 처리의 목적과 수단을 결정하는 자연인이나 법인, 공공기관, 그 밖의 기관을 말한다."고 정의하고 있다.

- 정보주체의 개인정보자기결정권
  - 개인정보처리자가 수행하는 자신에 관한 개인데이터의 처리과정에 참여하여 그 처리를 감시하는 권리이다. 개인정보처리자가 그 처리하는 개인정보에 대해 오·남용이 있는지를 감시하고, 위법한 처리가 있을 때 시정을 요구하거나 피해를 구제할 수 있게 하는 권리이다.

  - 나에 관한 데이터가 누구에 의해서 어떻게 수집, 이용, 제공되고 있는지를 알 권리(열람청구권), 분명한 처리 목적을 설정하고 그 목적 달성에 필요한 만큼의 정보만을 처리하도록 요구할 권리, 정보의 정확성과 최신성을 유지하기 위하여 틀린 정보나 낡은 정보를 수정하거나 삭제를 요구할 권리, 권한 없는 자에 의한 정보 접근을 제한하고 부당한 누출의 방지를 요구할 권리 등

개인정보보호법, 신용정보법의 동의 제도

- 개인 : EU GDPR 보호 모델
  - 정보주체의 동의, 계약의 이행, 법적 의무의 이행, 정보주체/자연인의 이익 보호, 정보 처리자/제3자의 정당한 이익, 민감데이터의 경우 사전 동의 원칙 적용(10가지 사항은 예외)
  - 열람청구권, 정정청구권, 삭제 청구권, 처리정지청구권, 사후적거부권, 자동 결정에 대한 이의 제기권, 데이터이동권

- 개인 : 한국의 보호 모델
  - 수집,이용 : EU GDPR 과 유사　　제공 : 사전 동의 원칙
  - 가명 정보의 경우 정보주체의 동의없이 수집, 이용, 제공 모두 가능
  - 열람청구권, 정정청구권(절대권), 삭제 청구권(절대권), 처리정지청구권(절대권)

- 신용 : 신용정보 회사들끼리 정보주체의 동의없이 제공
  - 추가 : 공개된 정보(SNS 정보)의 수집 및 처리 가능

보건의료 개인정보

- 보건의료 개인정보
  - 보건의료 개인정보의 경우 익명(anonymization)화 불가능
  - 다른 정보와 결합 시 개인 식별이 쉬운 정보임
  - 따라서, 개인정보 주체의 동의와 정보 활용 범위와 내용에 대한 고지는 필수

  - 가명 정보라 하여도 통계 작성(기업의 시장조사 등 상업적 목적 포함), 과학적 연구(제약사, 의료기기사, 보험사 등의 연구 목적 포함)의 개인정보 활용은 의료 시장화, 민영화로 이어질 가능성이 큼
  - 공익적 목적이라도 민감정보(유전정보, 개인 의료기록 및 건강정보 등)의 경우 별도의 보호장치가 있어야 함.

  - 특히. 건강보험공단과 심평원이 개인정보의 동의 없는 데이터를 민간에 제공하는 것은 심각한 문제임.

마이데이터 사업 성공을 위한 제언(1)

- 마이데이터 거버넌스 프레임워크
  - 데이터의 수집, 이용, 제공, 연계 등 전반에 걸쳐 개인정보의 활용과 보호의 균형을 맞출 수 있는 마이데이터 거버넌스 프레임워크 필요
  - **프레임워크 : 배경, 문제, 목적을 바탕으로 한 계획의 기본 이미지를 작성하여 목표, 수단을 생각하고, 개략적인 계획을 세우는 작업**

- 마이데이터 거버넌스 기구
  - 해외 ▶정보 거버넌스 기구 – 개인정보의 활용 및 보호와 관련된 전반적인 원칙과 정책 관장 ▶ 프로젝트 승인 기구 – 연구의 학술적 가치가 프라이버시 침해 위험성보다 큰지 등과 같은 심사기준에 따라 신청서를 검토, 승인 여부 결정 ▶ 연구윤리위원회 – 개인정보 문제를 넘어 연구의 윤리적 이슈 검토
  - 스코틀랜드 : 공익과 프라이버시 패널(PBPP), 영국 ADRN

  - 데이터의 수집, 이용, 제공과 관련한 구체적인 원칙, 정책, 절차 등을 가이드라인이나 매뉴얼로 정리, 공개

마이데이터 사업 성공을 위한 제언(2)

- **마이데이터 허브**
  - 연구자를 대신하여 데이터 보유기관과 데이터 접근에 대해 협의하고, 데이터 보유기관에 법적 자문을 제공. 데이터 보유기관으로부터 데이터를 제공받아 안전하게 보유, 관리하고, 연구자가 안전한 환경에서 데이터에 접근할 수 있도록 하는 역할
  - 데이터 보유기관 사이의 조정, 데이터 표준의 수립이나 품질의 관리, 데이터에 대한 보안, 데이터 연계 방법의 개발 등 역할 수행
  - 개인정보의 표준화를 통한 통합뷰어(플랫폼) 제공, 정보주체의 개인정보 이동 및 제공 내역 제공, 개인정보의 활용을 통한 서비스별 편익 및 위험 정보 제공 등
  - 연합형(federated type) : 데이터를 받아 접근을 매개, 중앙형(centralized type) : 데이터를 받아 보유, 관리

- 데이터 연계 모델
  - 국내 : 데이터 보유기관이 연계키를 생성하고, 연계된 데이터를 다시 데이터 보유기관에 제공
  - TTP(신뢰할 수 있는 제3자) 모델 : 데이터 연계 및 접근을 제공하는 기관과 연계키를 생성하는 기관을 분리
  - 방화벽 단일 센터 모델 : 각 기능을 담당하는 부서의 엄격한 분리 원칙

마이데이터 사업 성공을 위한 제언(3)

- 안전조치
  - 데이터의 수집, 저장, 연계, 제공 등 전 과정에 걸쳐서 개인정보 보호 및 보안을 위한 조치 필요
  - 연구자(safe people) 및 연구기관의 자격요건 명시
  - 연구 프로젝트(safe project) : 개인정보 침해 위험성보다 공익적, 학술적 가치가 있는지 평가
  - 환경(safe environment), 데이터(safe data) : 안전한 시설, 엄격한 보안 조치, 전과정 기록, 원격 접근의 경우 인증, 보안 접근, 로그 기록 모니터링 등
  - 결과물(safe results) : 공개되기 전에 전문가에 의해 철저하게 검토
  - 비식별 조치 및 프라이버시 영향 평가 수행

- 투명성과 시민 참여
  - 원칙과 절차, 사업 내용에 대한 정보의 투명 공개, 정책 결정 과정에 시민들과 다양한 이해당사자들의 참여 보장
  - 전반적인 마이데이터 거버넌스 체제의 구축과 이를 위한 충분한 사회적 논의 필요

나가기

데이터의 수집, 이용 및 제공 과정 전반에 걸쳐서 개인정보 보호 및 보안이 지켜지고 있다는 것에 대한 일반 시민의 신뢰가 가장 중요