2021 경제학공동학술대회 한국금융학회 세션 (분과A)
2021.2.5(Fri.) 발표자료

개인정보 활용 관련 법적 이슈의 연구

- 건강정보의 상업적 활용을 중심으로 -

발표자: 양기진 (전북대학교)

데이터 3법의 일괄 개정/시행

- 개인정보법 등 데이터 3법의 개정/시행
  - 2020.1.9. 국회 일괄가결, 2020.2.4. 공포(개정일), 2020. 8. 5. 시행
  - 개인정보 보호법 (약칭: 개인정보법)
  - 신용정보의 보호 및 이용에 관한 법률 (약칭: 신용정보법)
  - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 (약칭: 정보통신망법)

데이터 3법의 개정 배경

- 기술 개발과 정보보호 필요성
  - 4차 산업혁명 시대의 도래
  - 빅데이터 처리기술의 발달 및 정보주체의 식별여지 커짐
- 데이터기업의 급성장과 데이터가치의 인식
- 개인정보의 산업적 활용 기반 마련 및 데이터산업 육성
  - 가명정보나 추가처리 개념의 부재 등 데이터의 원활한 유통 곤란
- 개인정보의 실효적 보호 제고 필요성
  - 개인정보 수집/제공 동의의 형식화
  - 개인정보 침해 다발과 이를 막지 못하는 법에 대한 비판
- EU 거주민 개인정보 이전에 관한 EU의 적정성 승인 필요
  - 부처별로 쪼개진 정보감독권한의 집중 등 필요

EU GDPR에의 부응

- EU의 GDPR (General Data Protection Regulation, 2016/679)의 시행
  - 2016.4.27. 채택 및 2018.5.25.부터 시행
  - a regulation in EU law
    - It supersedes the Data Protection Directive 95/46/EC
  - It regulates
    - data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).
    - the export of personal data outside the EU and EEA areas.

- 정보이전에 관한 'EU 의회의 적정성 승인'을 획득하여야 한국기업의 데이터 활용이 용이해질 것임!

진행 개관

- 기본개념
- 개정법의 주요내용
- 업권별 부수업무 법제 정비
- 개정법 하의 데이터 결합
  - 특히 비신용정보와 금융정보의 결합에 대한 법규 적용 이슈
    - 민감한 개인정보를 가명처리 후 결합에 제공 가부
    - 과학적 연구*의 해석

      * 가명조치한 비신용 개인정보를 타인 보유 정보와 결합을 허용
    - 현행법상 신용정보의 범위 설정의 타당성 여부
  - 이상의 논점 관련 EU GDPR 및 미국 관련 법제 (HIPPA및 California법)
- 향후 법 개선방향

기본개념: 개인(신용)정보

- 개인정보 (개인정보법 제2조제1호)
  - 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당
    - 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 나목을 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보")
- 개인신용정보 (신용정보법 제2조제2호)
  - 기업 및 법인에 관한 정보를 제외한 살아 있는 개인에 관한 신용정보로서,
  - (i) 해당 정보의 성명, 주민등록번호 및 영상 등을 통하여 특정 개인을 알아볼 수 있는 정보, 또는 (ii) 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보임

기본개념: 신용정보

- 신용정보법상 '신용정보'
  - 금융거래 등 상거래에서 거래 상대방의 신용을 판단할 때 필요한 다음 각 목의 정보
  - 가. 특정 신용정보주체를 식별할 수 있는 정보
    - 이하 나목부터 마목까지의 어느 하나에 해당하는 정보와 결합되는 경우만 신용정보에 해당
  - 나. 신용정보주체의 거래내용을 판단할 수 있는 정보
    - 신용공여, 할부거래 등
    - **상법 제46조에 따른 상행위에 따른 상거래의 종류, 기간, 내용, 조건 등에 관한 정보 등**
  - 다. 신용정보주체의 신용도를 판단할 수 있는 정보
    - 금융거래 등 상거래와 관련하여 발생한 채무의 불이행, 대위변제, 그 밖에 약정한 사항 불이행 사실 관련 정보 등
  - 라. 신용정보주체의 신용거래능력을 판단할 수 있는 정보
    - 개인의 직업・재산・채무・소득의 총액 및 납세실적 등
  - 마. 가목부터 라목까지의 정보 외에 신용정보주체의 신용을 판단할 때 필요한 정보
    - 개인신용평점, 기업신용등급
    - 사회보험료 정보 등
    - 신용조회기록
    - **체납정보, 부동산등기부 기록정보 등**

기본개념: 처리/가명처리

- 처리 (개인정보법 제2조제2호)
  - 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위
- 가명처리 (개인정보법 제2조제1의2호)
  - 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것
- 가명처리 (신용정보법 제2조제15호)
  - 추가정보를 사용하지 아니하고는 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리하는 것임
  - 이 때의 처리에는 다음을 포함
    - 그 처리 결과가 (i) 어떤 신용정보주체와 다른 신용정보주체가 구별되거나 (ii) 하나의 DB(정보집합물)에서나 서로 다른 둘 이상의 DB 간에서 어떤 신용정보주체에 관한 둘 이상의 정보가 연계되거나 연동되는 경우 등에 해당하지만,
    - 그 추가정보를 분리하여 보관하는 등 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리한 경우

기본개념: 개인정보처리자 등

- 개인정보법 (일반법)
  - 개인정보처리자
    - 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등 (개인정보법 제2조제5호)
- 신용정보법
  - '신용정보회사등'
    - 신용정보회사, 본인신용정보관리회사, 채권추심회사, 신용정보집중기관 및 신용정보제공·이용자를 말함 (신용정보법 제15조제1항)
    - '신용정보제공·이용자'
      - 고객과의 금융거래 등 상거래를 위하여 본인의 영업과 관련하여 얻거나 만들어 낸 신용정보를 타인에게 제공하거나 타인으로부터 신용정보를 제공받아 **본인의 영업에 이용하는 자**와 그 밖에 이에 준하는 자(체신관서, 상호저축중앙회, 공제조합 등) (신용정보법 제2조제7호 및 시행령 제2조제18항)

개정 개인정보법의 주요내용

	주요내용
가명처리 개념의 정립	•가명처리는 개인정보의 일부 삭제 또는 대체하는 방법으로 추가 정보 없이는 특정개인을 식별할 수 없도록 처리하는 것을 의미 •익명처리가 가능한 경우 익명으로, 익명처리를 통해 목적을 달성할 수 없는 경우 가명에 의해 처리될 수 있도록 허용
가명정보의 처리에 관한 특례 조항 신설	•가명정보를 제3자에게 제공하는 경우 특정 개인을 식별할 수 있는 정보의 포함을 금지 •가명정보의 결합은 지정된 전문기관에서만 수행 •가명정보에 대한 안전조치 의무, 특정개인 식별을 위한 가명정보 처리 금지, 가명처리 위반 시 전체 매출액의 3/100 과징금 부과
정보통신망법 규정 이관	•정보통신서비스 제공자 등의 개인정보 처리 특례 이관 - 정보통신망법의 "개인정보의 보호(제4장)" 규정
개인정보보호 위원회 위상 강화	•개인정보보호위원회의 지위 격상: 대통령 직속 → 중앙행정기관 •구성: 15명(위원장1명/상임위원1명) → 9명(위원장1명/부위원장1명) •임기: 3년 (1회 연임) •권한: 심의·의결, 조사·처분권, 가이드라인에 대한 관리·감독 기능

정희수
(2020.7.24.)
4면

개정 신용정보법의 주요내용 1/2

	주요내용
가명정보의 정의 및 위반시 제재 강화	•정보 특성에 대한 정의 명확화 - 개인정보: 특정개인에 관한 정보, 개인을 알아 볼 수 있는 정보 - 가명정보: 추가정보 없이 특정 개인을 식별할 수 없게 조치한 정보 - 익명정보: 개인을 식별할 수 없게 조치한 정보 •규정 위반 시(고의적 재식별 포함) 과징금 대상 범위 확대 : 위반행위 관련 매출액의 3/100 이하 → 전체 매출액의 3/100 이하 •정보결합 위반, 고의적 재식별: 5년이하 징역 또는 5천만원이하 벌금 •가명(익명) 미처리 정보 전달, 분리보관 위반: 5천만원 이하 과태료
신용정보산업 (CB)의 인가 단위 개편	•특화CB사 신설: 비금융정보 전문 CB, 개인사업자 CB •겸영업무: 신용정보업, 채권추심업, 본인확인기관 업무 등 •부수업무: 개인신용평가 결과 본인 제공, 정보의 본인 및 제3자 제공, 가명(익명)정보의 이용 및 제공, 개인신용정보/기타 정보에 기초한 데이터 분석/컨설팅 업무 •영업행위 규제 신설 •개인CB사, 개인사업자CB사 등에 대한 최대주주 적격성 심사제 도입

정희수
(2020.7.24.)
6면

개정 신용정보법의 주요내용 2/2

본인신용정보 관리업 도입	•요건: 최소자본금 5억원, 금융회사 출자요건 미적용 •대상: 은행 예금, 증권 예탁금/CMA, 은행 대출, 카드/할부금융/리스 거래 내역, 보험 계약 및 청구/지급 정보, 투자상품 등 •겸영업무: 투자자문업 또는 투자일임업 •부수업무: 본인 신용정보에 기초한 데이터의 분석/컨설팅 업무, 정보계좌 제공 업무, 정보정정청구 등 권리대리행사 업무 •정보제공 방식: 정보제공의 안전성과 신뢰성이 보장되는 방식(API) 중계기관을 통한 정보 전송 허용, 정기적인 전송 시 수수료 부담 可
데이터전문기관 지정	•업무: 정보의 결합 및 전달, 익명처리의 적정성 평가 •적정성평가위원회 설치 허용 및 위험관리체계 마련
신용정보주체의 보호 조치	•정보활용동의 등급제: 정보활용 동의 시 정보제공에 따른 사생활 침해 위험, 소비자 이익이나 혜택 등을 평가해 등급 산정 •정보 활용/관리 실태 상시평가제: 금융위에서 관리실태 점검 결과를 점수(등급)화하고 감독원의 검사에 활용 •개인신용정보의 전송요구권: 본인 정보를 정보주체 본인, 본인신용정보관리회사, 신용정보제공자/이용자, 개인신용평가회사 등에 요구 (단, 컴퓨터 등 정보처리장치로 처리된 신용정보에 한정) •프로파일링 대응권: 자동화 평가 결과에 대한 설명/이의제기 허용 •개인신용평점 하락 가능성에 대한 설명의무

정희수
(2020.7.24.)
6면

개정 데이터3법 하의 정보 결합

- 금융정보와 비신용정보의 결합 이슈
  - 금융정보는 통상 신용정보법상 신용정보의 범주에 해당할 것임
    - 금융관련법상 금융정보의 정의는 안 보임
- 보유주체가 다른 개인정보 DB(정보집합물)간 결합 근거
  - 신용정보DB간 결합근거: 신용정보법 제17조의2
    - 데이터전문기관에 의하여 신용정보회사등이 보유하는 정보집합물과 제3자가 보유하는 정보집합물 간의 결합 및 전달
  - 개인정보DB간 결합근거: 개인정보법 제28조의3
    - 개정위 등이 지정하는 전문기관이 가명정보 형태, 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합 허용
  - 개인정보DB와 신용정보DB 간의 결합은?

개정 데이터3법 하의 논란

- 금융정보와 비신용정보의 결합 이슈
  - 신용정보법 제17조의2 vs 개인정보법 제28조의3
  - <논란> 비신용정보(특히 민감정보)와 금융정보의 결합은 제약없이 가능한가
    - (1) 비신용정보 중 민감정보도 가명처리하여 결합에 제공 가능하다고 해석할 수 있을 것인가.
    - (2) 비신용정보(가명정보 형태)를 다른 정보와 결합시키는 것을 허용하는 사유인 통계작성, 과학적 연구, 공익적 기록 보존 등을 어떻게 해석할 것인가.
      - 결합가능여부 판단시 과학적 연구를 산업적 연구로 널리 확대할 수 있는가.
    - (3) 결합대상인 정보의 성격은 신용정보인가, 비신용정보인가.
      - 현행법상 신용정보 범위 설정은 타당한가.

민감정보 중 건강정보 처리

- 민감정보 (개인정보법 제23조제1항)
  - 사상・신념, 노동조합・정당의 가입・탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보
- 처리 허용여부
  - 민감정보의 처리 제한 및 예외적 처리* 허용 (개인정보법 제23조제1항)
    - * ① 정보주체의 별도 동의, ② 법령상 근거
  - 개인정보법 제28조의2은 민감정보의 제한없는 처리근거가 될 수 있는가.
    - 개인정보법 제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, **과학적 연구**, 공익적 기록 보존 등을 위하여 정보주체의 동의 없이 **가명정보**를 처리할 수 있다.
    - 개인정보법 제2조 제8호: "과학적 연구"란 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 말한다.
- 논점
  - 논점 1: '민감정보'를 타법의 제한에 불구하고 처리 가능한가.
  - 논점 2: '과학적 연구'의 범위를 어떻게 해석할 것인가.

민감정보인 건강정보의 처리

- 민감정보인 건강정보의 처리 제한
  - 대표적인 민감정보
    - 단, 가명처리 행위 자체는 보안성을 높이므로 정보주체의 명시적 동의 없이도 허용 (추가처리 등)
  - 타인에게 제공 또는 원수집목적 외의 다른 목적으로 이용 가능한가.
    - 타법상 의료정보의 처리 제한
      - 정보 누설 금지 (의료법 제19조), 환자외 기록열람 엄격 제한 (의료법 제21조)
      - 직무상 목적 외 용도로의 개인정보 제3자 제공 금지 (국민건강보험법 제102조)
    - 개인정보법의 후순위적 적용
      - 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다. (법 제6조)
    - 개인정보법은 의료법보다 우선적용되기 어려움!
  - 건강정보의 활용 관련 논란
    - 건강정보를 가명처리하여 '처리'(제3자 제공등)할 수 없다는 의견 등 <건치 신문 (2020.9.2.)>

개인정보법 적용관련 파생 논점

- 파생되는 문제점
  - 신용정보법과 달리, 개인정보법의 가명정보 처리허용 목적 범위는 협소
    - 개인정보법은 산업적 연구나 상업적 통계 목적의 정보처리를 허용하는 명시적 근거를 두지 않음
    - Cf. 통계작성, 과학적 연구, 공익적 기록보존 등 (개인정보법 제28조의2 제1항)
  - 따라서 비신용 개인정보와 금융정보를 결합할 경우에 관한 법적 불확실성이 존재
    - 각종 금융산업에서 맞춤형 금융상품 설계·판촉에 관심이 많을 것임
  - <의문> [정부의 해석과 상관없이] 비신용 개인정보인 건강정보를 가명처리한 후 독자적으로 또는 금융정보DB와 결합하여 신용정보회사등이 [산업적] 연구목적, [상업적] 통계작성 목적으로 이용하는 것이 타당할지
    - 건강정보 외 다른 비신용 개인정보에도 동일한 논의 가능

건강정보 처리 관련 정부 입장

- 최근「보건의료 데이터활용 가이드라인」의 제정
  - 제정배경 (행안부&복지부)
    - 의료데이터의 비식별조치 통한 산업적 활용의 법적 근거 미비
    - 제약이나 의료기기 등 기술, 제품 개발에 데이터 활용 불가
    - 의료데이터활용 및 민간개방 확대 필요
    - 보건의료 분야의 개인정보 가명처리, 결합, 활용절차 등의 필요
  - 2020.9월 제정
- 적용순위
  - 보건의료 데이터활용 가이드라인 > 개인정보 가명처리 가이드라인
    - 개인정보 보호위원회, “개인정보 가명처리 가이드라인” (2020.9월)
- 주된 내용
  - 보건의료 데이터의 가명처리 절차, 필요 보안조치
  - 가명정보 활용 및 제3자 제공시 절차 및 가버넌스
  - 가명정보 활용시스템 요건 등

정부 입장: 보건의료 데이터활용 가이드라인

- 민감정보인 건강정보의 활용 허용
  - 건강정보 활용 허용 (원칙)
    - '가명처리' 후 정보주체의 동의 없이 목적 제약없이 활용 가능
  - 예외: 정보주체의 동의 필요
    - (1) '인권 및 사생활보호에 중대 피해 야기 가능한 일부 건강정보'의 활용시 동의 원칙
      - 예컨대, 정신질환 및 처방약 정보, 성매개감염병 정보, 후천성면역결핍증 정보, 희귀질환 정보, 학대 및 낙태 관련 정보
    - (2) 안전한 가명처리 존재시에만 가명처리하여 건강정보를 활용
      - 음성정보 등과 같이 안전한 가명처리 방법이 개발되지 않은 경우에는 정보주체 동의하에서만 활용

개인정보법 제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 **가명정보**를 처리할 수 있다.

가이드라인상 건강정보

- 가이드라인의 적용대상인 '건강정보' (보건복지부, 2020.9.25. 제정)
  - 의료법상 진료기록부 및 전자의무기록, 그밖에 병원 내에서 생산되어 진료내역을 표시하고 있거나 쉽게 추정할 수 있는 기록
    - 진료내역을 담은 병원 영수증 등
  - 건강보험공단, 건강보험심사평가원, 기타 민간보험사 등에서 수집한 보험청구용 자료, 가입설계에 사용된 건강·질병·상해 등 관련 자료 및 그 부속자료
  - 건강검진자료, 건강검진결과 정보
  - 의사에 의해 진단되거나, 의료기기에 의해 계측되거나, 보험청구기록, 기타 알고리즘 등의 추정을 통해 파악·추정한 건강상태 정보
  - 건강상태 또는 건강습관 여부·정도를 측정하기 위해 기기를 통해 수집한 정보
    - (예시 : 걸음 수, 심박 수, 산소포화도, 혈당, 혈압, 심전도)
  - 특히, 일반적으로는 건강정보로 보기 어렵지만, 질환의 진단·치료·예방·관리 등을 위해 사용되는 정보는 건강정보로 봄
    - (예시) 음성녹음은 평시에는 건강정보가 아니지만, 이를 통해 각종 질환의 위험도를 예측할 경우 해당 음성녹음 파일도 건강정보로 봄

가이드라인상 과학적 연구 범위

- 보건의료 데이터활용 가이드라인상 '과학적 연구'의 범위
  - 자연과학적인 연구
  - 과학적 방법을 적용하는 역사적 연구나 공중보건 분야에서 공익을 위해 시행되는 연구 등
  - **새로운 기술·제품·서비스의 연구개발 및 개선 등 산업적 목적의 연구 포함**

√ *누구의 이익을 위한 것인가?*

[보건의료 분야 과학적 연구의 예시]

- 약물을 개선·개발하거나, 기존 약물의 효과를 평가하기 위한 연구
- 의료기기를 개선·개발하거나, 기존 의료기기의 효과를 평가하기 위한 연구
- 진단·치료법을 개선·개발하거나, 기존 진단·치료법의 효과를 평가하기 위한 연구
- 진단·치료 등의 의료적 목적을 갖는 소프트웨어를 개선·개발하거나, 기존 의료적 목적을 갖는 소프트웨어의 효과를 평가하기 위한 연구
- 건강상태 모니터링, 운동지도 등의 비의료적 건강관리 목적을 갖는 소프트웨어를 개선·개발하거나, 기존 비의료적 건강관리 목적을 갖는 소프트웨어의 효과를 평가하기 위한 연구
- 특정 질환을 갖고 있거나, 특정 치료제·치료법에 적합한 임상적 요건을 갖춘 환자의 수, 지역적·연령적 분포 등을 살피는 연구, 타 질환과의 연관성을 살피는 연구
- 다양한 약물, 치료법, 진단법 등 상호간의 의학적·사회적 효용을 비교하는 연구
- 인구집단 내 건강상태의 지역적·직업적 분포, 사회적 여건 등의 편차를 살피는 등의 연구
- 보건의료 데이터를 표준화하거나, 품질을 높이거나, 안전하게 보호하는 등 보건의료 데이터를 원활히 관리하기 위한 기술·소프트웨어를 개발하기 위한 연구

가이드라인과 의료법간 간섭

- 「의료기관 개설 및 의료법인 설립 운영 편람」(발췌)
  - Ⅰ 개인정보 보호법과의 관계
  - 1. 개인정보 보호법 제6조
    - 개인정보 보호법 제6조에 따라, 의료기관이 보유하는 환자에 관한 기록(정보)에 대해 의료법 우선 적용
      - 개인정보 보호법 제6조(다른 법률과의 관계) 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.
  - 2. 의료법 우선 적용
    - ⅰ)의료기관이, ⅱ)보유 중인 ⅲ)환자에 관한 기록을 ⅳ)제3자(외부자)에게, ⅴ)열람 또는 사본 발급 등 그 내용의 확인을 제공하는 경우에 개인정보 보호법을 적용하지 않고 의료법*을 적용함
      - 의료법 제21조 또는 제21조의2 규정 등 적용
    - 따라서 개인정보 보호법에서 제3자 제공이 허용되는 경우라도 의료법 제21조 또는 제21조의2에서 정하는 경우가 아니면 환자에 관한 기록과 관련한 정보를 제3자에게 제공 금지
  - 3. **개인정보 보호법이 적용되는 경우(의료법 적용하지 않음)**
    - **가명처리하여 환자식별력이 없는 진료기록(정보)**
    - 의료기관이 아닌 자(또는 기관)가 보유하는 진료기록(정보)
      - 예시) 의료기관이 아닌 환자가 보관

보건의료 데이터활용 가이드라인, 34면

추가처리로 제공가능할까

- 동의 요하지 않는 추가처리 (further processing)
  - 개인정보법 (법 제15조제4항, 시행령 제14조의2 제1항)
    - 법률: 당초 수집 목적과 '**합리적으로 관련된**' 범위에서
    - 시행령: 당초 수집목적과 추가된 이용·제공 목적과의 **관련성** cf. 1차 입법예고 시행령
  - 신용정보법 (법 제32조제6항 제9의4호)
    - 당초 수집한 목적과 '**상충되지 아니하는**' 목적으로 개인신용정보 제공시
      - 가. 양 목적 간의 관련성
      - 나. 신용정보회사등이 신용정보주체로부터 개인신용정보를 수집한 경위
      - 다. 해당 정보의 제공이 신용정보주체에게 미치는 영향
      - 라. 해당 정보에 대하여 가명처리를 하는 등 신용정보의 보안대책 적절 시행 여부

추가처리: 양법의 비교

개인정보법	신용정보법
법 제15조(개인정보의 수집·이용) ④ **개인정보처리자는** 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 제공할 수 있다. 시행령 제14조의2(개인정보의 **추가적인 이용·제공**의 기준 등) ① 개인정보처리자는 법 제15조제3항 또는 제17조제4항에 따라 정보주체의 동의 없이 개인정보를 이용 또는 제공(이하 "개인정보의 추가적인 이용 또는 제공"이라 한다)하려는 경우에는 다음 각 호의 사항을 모두 고려해야 한다. 1. 당초 수집 목적과 상당한 관련성이 있는지 여부 2. 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부 3. 정보주체의 이익을 부당하게 침해하는지 여부 4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 ② <생략>	법 제32조(개인신용정보의 제공·활용에 대한 동의) ⑥ **신용정보회사등**(제9호의3을 적용하는 경우에는 데이터전문기관을 포함한다)이 개인신용정보를 제공하는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 제1항부터 제5항까지를 적용하지 아니한다 <정보주체의 동의 없이 제공 가능>. <중략> 9의4. 다음 각 목의 요소를 고려하여 당초 수집한 **목적과 상충되지 아니하는** 목적으로 개인신용정보를 제공하는 경우 가. 양 목적 간의 관련성 나. 신용정보회사등이 신용정보주체로부터 개인신용정보를 수집한 경위 다. 해당 개인신용정보의 제공이 신용정보주체에게 미치는 영향 라. 해당 개인신용정보에 대하여 가명처리를 하는 등 신용정보의 보안대책을 적절히 시행하였는지 여부

추가처리 허용의 범위(further processing)

- GDPR Recital 50
  - 개인정보가 최초로 수집된 정보 '이외'의 목적으로 정보주체의 동의 없이 해당 정보를 처리(further processing)하려면, 해당 처리가 해당 개인정보가 원래 수집된 목적과 **'양립 가능한(compatible)'** 경우이어야 함
    - The processing of personal data **for purposes other than those** for which the personal data were **initially collected should be allowed only where the processing is compatible with the purposes** for which the personal data were **initially collected.** [2]In such a case, no legal basis separate from that which allowed the collection of the personal data is required
- 한국 법원의 태도
  - **공개개인정보**에 관한 목적제한 원칙 적용
    - 이미 공개된 개인정보라도 해당 정보의 수집이나 제3자 제공 등을 허용할 경우 **'객관적으로 보아 정보주체가 동의한 범위 내에서 처리하는 것으로 평가할 수 있는 경우'로 한정** (대법원 2016. 8. 17. 선고 2014다235080 판결)
  - 공개된 정보라도 목적제한 원칙상 애초에 공개된 목적에 부합하는 방식으로 활용

보호대상 개인정보: 식별가능성

- 법의 보호대상인 개인정보의 범위
  - 개인(신용)정보 중 '가명정보'
    - 개인정보법: 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.
    - 신용정보법: 기업 및 법인에 관한 정보를 제외한 살아 있는 개인에 관한 신용정보로서, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보
  - 식별가능성의 판단
    - 누구의 관점에서 식별가능성의 존부를 판단할 것인가
    - 가명처리 가이드라인 (2020.9월): 상대설
      - 개인정보에 대한 판단기준은 **'가명정보처리자'가 보유하는 정보 또는 접근가능한 권한 등 상황에 따라 달리 판단** (가이드라인3면); 해당정보를 처리하는 자(정보의 제공 관계에 있어서 제공받은 자를 포함) (가이드라인 18면)
    - GDPR: 절충설
      - 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 amount of time required for identification, taking into consideration the available technology at the time of the processing** and technological developments.

- 추후 법 개선사항
  (개인정보 활용과 개인의 권리의 조화)

연구(research)의 범위

- 개인정보법
  - 통계작성, **과학적 연구**, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리 가능(제28조의2 제1항)
    - 개정전 개인정보법: 통계작성 및 **학술연구** 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우 정보주체의 동의 없이 제3자에게 제공가능(법 제18조 제2항 제4호)
  - 「보건의료 데이터 활용 가이드라인」의 확대 해석
    - 대부분의 건강정보에 대하여 '가명처리 ' 를 전제로 처리를 허용 (수집목적 외 처리, 제3자 제공 등)
- 신용정보법
  - **산업적** 연구를 포함하며 상업적 목적의 통계 포함 (제32조제6항제9호의2) <신설>
- GDPR
  - further processing for archiving purposes in the public interest, **scientific or historical research purposes** or **statistical purposes** shall, in accordance with Article 89(1), **not be considered to be incompatible with the initial purposes.**(Art.5(1)(b))

GDPR: 민감정보 처리의 원칙적 금지

- GDPR Recital (51)
  - 우선 GDPR은 민감정보를 가명처리하여 수집목적 외 활용 또는 제3자 제공하는 명시적 규정을 두지 않음
  - **Personal data which are, by their nature, particularly sensitive** in relation to fundamental rights and freedoms merit specific protection **as the context of their processing could create significant risks** to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, …<중략>
  - **Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation,** taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing.
  - **Derogations from the general prohibition for processing such special categories** of personal data **should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular** where the processing is carried out **in the course of legitimate activities** by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

GDPR: 민감정보 처리 허용요건

- GDPR Recital (52)
  - 민감정보의 처리에는 EU법 또는 회원국법에 근거를 두고 적절한 보호장치를 두어야 하며 또한 처리를 허용할 **공익(public interest)**이 필요
    - **Derogating from the prohibition on processing special categories of personal data** <민감정보> **should also be allowed when** provided for **in Union or Member State law and subject to suitable safeguards,** so as to protect personal data and other fundamental rights, where it is **in the public interest to do so,** in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, **the prevention or control of communicable diseases and other serious threats to health.**
  - 구체적인 민감정보 처리의 허용 사유로, 공중 위생(public health) 및 건강관리서비스의 운영을 포함하는 보건 목적(health purpose)이 거론될 수 있으며, **보건 목적을 위한 처리 허용은** 특히 건강보험시스템의 혜택 청구 절차의 품질과 비용절감을 위하여, 또는 공익, 과학적 또는 역사적 연구 또는 통계 목적을 위하여 행해질 수 있음
    - **Such a derogation may be made for health purposes, including public health and the management of health-care services,** *especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims* ***for benefits and services in the health insurance system,*** *or* ***for archiving purposes in*** *the public interest,* ***scientific or historical research purposes or statistical purposes.*** A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

EDPS: 과학적 연구의 해석

- 유럽 데이터 보호 감독자 (EDPS)*의 사전 의견서
  - * EDPS는 EU의 독립적인 데이터 보호 당국
  - For the purposes of this Preliminary Opinion, the special data protection regime **for scientific research** is understood to apply **where each of the three criteria are met:**
    - 1) personal data are processed;
    - 2) relevant sectoral standards of methodology and **ethics apply, including the notion of informed consent, accountability and oversight;**
    - 3) the research is carried out **with the aim of growing society's collective knowledge and wellbeing, as opposed to serving primarily one or several private interests.**
  - Under the GDPR, the role of research is understood to provide knowledge that can in turn **'improve the quality of life for a number of people and improve the efficiency of social services'. …** It is a common assumption that **scientific research is beneficial to the whole of society and that scientific knowledge is a public good** to be encouraged and supported.
  - The Article 29 Working Party, in its guidelines on consent, understood scientific research as a 'research project set up in accordance with **relevant sector-related methodological and ethical standards**'.

European Data Protection Supervisor (EDPS) (Jan. 6, 2020), pp.11-12

Scientific research purposes의 맥락 중시

- Scientific research purposes: Recital (159)
  - 과학적 연구 목적의 개인정보 처리의 범위
    - 기본/응용연구나 민간펀드 연구도 포함 (주체 널리 포섭)
    - 공중위생 부문에서 공익을 위하여 수행되는 연구도 포함되어야 함 (연구결과의 향유 ○)
  - 과학적 연구 목적상 개인정보 처리가 허용되려면 개인정보의 공개 관련 특정 요건(specific conditions)이 적용되어야 함, 이 때 특히 보건(health)의 맥락에서 과학적 연구의 결과가 해당 정보주체의 이익에 부응하는 경우 GDPR에 합치될 수 있음 *[해석 보정]*
  - Where personal data are processed **for scientific research purposes,** this Regulation should also apply to that processing. For the purposes of this Regulation, 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. Scientific research purposes should also **include studies conducted in the public interest in the area of public health.**
  - **To meet the specificities** of processing personal data **for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context** gives reason for further measures **in the interest of the data subject,** the general rules of this Regulation should apply in view of those measures.

GDPR: 과학적 연구
- 적법한 추가처리의 일종 -

- GDPR은 과학적 연구등 목적 허용 근거
  - 과학적 연구 등의 목적에 의한 처리를 '추가처리'의 일종으로 보고 과학적연구 등 목적에 의한 처리를 [원수집목적과] 양립가능한 '적법'한 추가처리로 간주
    - GDPR Recital 50. **Further processing for** archiving purposes in the public interest, scientific or historical **research purposes or statistical purposes** should be considered to be **compatible lawful processing operations.**
  - 추가처리가 원 수집목적과 양립가능한 '적법'한 추가처리가 되려면, 목적간 관련성, 수집당시의 맥락(정보처리자의 관계등 고려), 해당 개인정보의 성격, 추가처리가 정보주체에 야기할 결과, 그리고 적정한 세이프가드의 존재가 동시에 충족되어야 함
    - GDPR Recital 50. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the **lawfulness of the original processing**, should take into account, inter alia: **any link between those purposes and the purposes of the intended further processing**; **the context** in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; **the nature** of the personal data; **the consequences of the intended further processing for** data subjects; and the existence of **appropriate safeguards** in both the original and intended further processing operations

미국: 개인의 건강정보 관련 규제

- 관련 법률: The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - HIPAA는 HHS의 장(the Secretary of the U.S. Department of Health and Human Services) (HHS)에게 일정한 건강정보(certain health information)의 프라이버시와 보안을 보호하는 규정 제정 권을 부여
- 관련 규정
  - HIPAA에 의거, HHS의 장이 Privacy Rule 및 Security Rule 제정
    - Privacy Rule (*Standards for Privacy of Individually Identifiable Health Information*)
      - 일정한 건강 정보의 보호에 관한 국가 기준을 정립
    - Security Rule (*Security Standards for the Protection of Electronic Protected Health Information*)
      - 전자적 형태로 보유 또는 이전되는 일정한 건강정보를 보호하는 국가적 보안 기준을 정립
  - 양자의 관계
    - Security Rule은 Privacy Rule상의 보호를 운영
    - Security Rule은 피규제자(covered entities)가 개인의 '보호대상인 전자적 형태의 건강정보(e-PHI)'의 보안을 위하여 두어야 하는 기술적/비기술적 세이프가드를 규율

US HHS.gov. 사이트

미국: HHS Privacy Rule

- 피규제자
  - Health Plans: 의료비를 제공/지출하는 개인 및 단체의 계획
  - Health Care Providers
    - 규모를 불문하고 일정 거래(HIPPA Transactions Rule 하의 청구 등) 관련 전자적 형태로 건강정보를 전송하는 모든 Health care provider를 지칭
  - Health Care Clearing houses
  - Business Associates 등
    - A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. HSS.gov.
- 보호대상 정보 (protected health information: PHI)
  - 개인을 식별할 수 있는 모든 건강 정보(all individually identifiable health information) &
    - 해당 개인의 과거, 현재 또는 미래의 신체적 또는 정신적 건강 또는 상태
    - 해당 개인에 대한 health care의 제공 또는
    - 해당 개인에게의 health care의 제공을 위한 과거, 현재 또는 미래의 지불정보
  - 개인의 식별가능성이 존재할 경우
    - 해당 개인을 곧바로 식별하거나 또는 해당 개인의 식별에 이용될 수 있다고 믿을 합리적인 근거(reasonable basis)가 있는 경우

US HIPAA Privacy Rule

PHI 미해당 정보

- 익명정보 (De-Identified health information)
  - 개인을 식별하지 않거나 개인 식별을 위한 합리적인 근거를 제공하지 않는 정보
    - 보호대상 아님
  - 적정한 익명조치 요건
    - (1) 적격 통계학자(qualified statistician)에 의한 공식적 결정 또는
    - (2) 아래 두가지 요건이 모두 구비된 경우에만(only if) 적정함
      - (i) 개인의 식별자 및 개인의 친적, 가족, 피용인 등의 식별자가 제거되고
      - (ii) 잔여 정보가 해당 개인의 식별을 위하여 사용될 여지가 있다는 점에 대해 피규제자 (covered entity)의 실제적 인식이 전혀 없는 경우

US HIPAA Privacy Rule

미국: PHI 이용 및 공개

- 기본 원칙
  - 피규제자가 PHI를 목적외 활용 또는 제3자 제공하려면, (1) Privacy Rule이 허용 또는 요구하는 경우, 또는 (2) 해당 정보주체인 개인이 서면으로 허락한 경우이어야 함
    - 목적외 활용(use of PHI): communicating that information within the covered entity.
    - 제3자 제공(disclosure of PHI): communicating that information to a person or entity outside the covered entity, or the communication of PHI from a health care component to a non-health care component of a hybrid entity.
- PHI의 공개의무 경우
  - 피규제자는 오직 다음 2개 상황에서만 공개의무 발생
    - (1) PHI에 대한 접근을 요구하는 해당 정보주체에게, 또는 (2) 법규 준수여부 조사 등을 수행하는 HHS에게
- PHI의 활용/제공이 허용되는 경우
  - (1) 해당 개인에게, (2) 치료, 지불, health care 적용, (3) **동의 또는 거절 기회의 부여**, (4) 기타 허용되는 이용/공개에 부수하여, (5) 공익 및 Benefit Activities, 그리고 (6) **연구, 공익 또는 health care 운영 목적을 위한 제한된 데이터셋(Limited Data Set)***

    * Limited data set이란, 일정한 특정 개인 및 그 친척, 가족구성원 및 피고용인들에 관한 직접적인 식별자가 제거된, 보호대상 건강정보(PHI)를 말함 (Privacy Rule (6))

US HIPAA Privacy Rule

미국: 연구 목적 PHI의 활용

- 연구 준비 활동에의 PHI (protected health information) 활용/제공
  - 연구 준비 관련 활동의 경우, 피규제자는 PHI를 활용/제공 가능
  - 생존 개인의 PHI 활용등 관련 엄격한 제약요건
    - (1) PHI에는 다음 식별자가 모두 제거되어야 함
      - 1. Names./ 10. Certificate/license numbers./ 2. Postal address information, other than town or /11. Vehicle identifiers and serial numbers, city, state, and ZIP Code. including license plate numbers./ 3. Telephone numbers./12. Device identifiers and serial numbers./ 4. Fax numbers./13. Web universal resource locators (URLs)./ 5. Electronic mail addresses./14. Internet protocol (IP) address numbers./ 6. Social security numbers./ 15. Biometric identifiers, including fingerprints/ 7. Medical record numbers. and voiceprints./8. Health plan beneficiary numbers. 16. Full-face photographic images and any/ 9. Account numbers. comparable images.
    - (2) 피규제자는 다음 사항에 관한 연구자 진술을 확보하여야 함
      - (i) 연구 프로토콜 준비 또는 유사한 연구준비 목적상 PHI의 이용/공개가 필요하며, (ii) 검토 과정 중 피규제자가 PHI를 계속 보유할 것이며, (iii) 이용/접근이 요청되는 PHI가 해당 연구에 필요함
  - 사망자의 PHI에 관한 연구
    - 사망자의 PHI를 연구용으로 활용/제공할 경우 동의 등을 얻을 필요는 없으나 사망자의 PHI에의 접근을 요청하는 연구자로부터 다음 진술을 확보하여야 함
      - (i) 사망자의 PHI에 관한 연구 목적으로만 해당 활용/제공되며, (ii) 해당 PHI의 활용이나 제공이 해당 연구 목적에 필요하며, (iii) 피규제자의 요청이 있는 경우 해당 연구자가 요청하는 PHI 관련 개인의 사망 확인 서류를 제출함

US NIH.gov.

미국: Privacy Rule상 Research purpose

- 연구란 지식을 개발하거나 지식의 일반화에 기여하려는 체계적인 조사를 말함
  - "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge.
- Privacy Rule은 피규제자가 개인의 승인 없이도 연구 목적 수행을 위하여 PHI를 목적외 이용 및 제3자 제공하는 것을 허용하나, 다음의 조건이 필요
  - The Privacy Rule permits a covered entity to use and disclose protected health information for research purposes, without an individual's authorization, provided the covered entity obtains either: (1) documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board; (2) representations from the researcher that **the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research**, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or (3) representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought.[38] A covered entity also may use or disclose, without an individuals' authorization, a limited data set of protected health information for research purposes (see discussion below).

미국: PHI 활용시 개인의 권리

- PHI가 연구에 활용될 경우 해당 정보주체인 개인의 권리 (Privacy Rule)
  - 연구에 활용/제공되는 PHI의 개인 정보주체에게 일정한 권리를 부여
    - 해당 개인은 피규제자 또는 그 협력업체(business associates)에 대하여 자신의 PHI에 관한 일정한 제공 기록(제공 기록: accounting of disclosure)을 얻을 수 있음 (연구자에 의한 공개 포함)
    - 피규제자는 PHI 관련 개인에게 해당 기관의 프라이버시 관행 및 개인의 프라이버시권에 대하여 서면통지로 알려야 함
  - 이 과정에서 개인이 갖는 권리
    - 개인은 health care 관련 일정한 기록에 관한 접근, 기록의 수정요구, 제약 설정 요구 및 비밀대화를 요구할 권한을 부여받으며,
    - 개인은 피규제자에 대하여 언제/왜 자신들의 PHI가 주체의 승인없이 제공되었는지에 관한 서면 기록을 요구하여 수령할 권리가 부여되며,
    - 개인은 Privacy Rule의 위반이 발생하였다고 믿을 경우에 피규제자 및 HHS의 장을 상대로 불만을 제기할 권리를 가짐
- 시사점
  - 건강정보를 처리(이용 내지 제3자 제공)할 경우에도, 개인인 정보주체에게 자신의 정보가 어떻게 이용/제공되었는지 내역을 살펴볼 권한을 확보해줄 필요

US HIPAA Privacy Rule

US: California Consumer Privacy Act of 2018

- 캘리포니아법상 소비자정보를 이용하는 Research의 적법 요건
  - 공익 요건, 연구가 개인정보가 수집된 사업목적과 양립가능할 것, 이용후 가명화 및 익명화조치를 취할 것, 원 수집동의받은 이용 목적과 양립가능한 연구에만 사용할 것, 일체의 상업적 목적 용도로는 사용 불허
  - California Consumer Privacy Act **1798.140.** For purposes of this title: (s) "Research" means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:
    - (1) **Compatible with the business purpose** for which the personal **information was collected.**
    - (2) **Subsequently pseudonymized and deidentified, or deidentified and in the aggregate,** such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.
    - (3) Made subject to **technical safeguards that prohibit reidentification** of the consumer to whom the information may pertain.
    - (4) ~ (6) <생략>
    - (7) **Used solely for research purposes that are compatible with the context in which the personal information was collected.**
    - (8) **Not be used for any commercial purpose.**
    - (9) Subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

US: California Consumer Privacy Act of 2018

- 캘리포니아법상 연구자의 거절권 (소비자의 개인정보 삭제 요청시)
  - 정보처리자가 정보삭제 요청을 거절할 수 있는 연구란, 공익 또는 동료 리뷰가 된 과학적, 역사적, 통계적 연구로서 모든 윤리 및 정보보호법을 좇는 것이어야 함
  - California Consumer Privacy Act **1798.105.**
  - (a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.
  - (d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:
    - (6) **Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws**, when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

참고: EU Copyright Directive상 과학적 연구

- The EU's 2019 Copyright Directive (Directive (EU) 2019/790)
  - EU 저작권지침은 과학적 연구 관련하여 수행'주체'를 구분
    - This Directive considers scientific research to cover 'both the natural sciences and the human sciences', and **distinguishes between not-for-profit and public interest bodies and organisations operating under commercial influences:**
  - 상기업이 결정적 영향력을 행사하는 조직이 연구를 행할 경우 해당 연구 결과에 우선적 접근권을 초래할 수 있으므로, 이 경우에는 동 지침상 연구조직(research organisations)으로 볼 수 없음
    - *Due to the diversity of such entities, it is important to have a common understanding of research organisations. They should for example cover, in addition to universities or other higher education institutions and their libraries, also entities such as research institutes and hospitals that carry out research. Despite different legal forms and structures,* ***research organisations*** *in the Member States* ***generally have in common that they act either on a not-for-profit basis or in the context of a public-interest mission recognised by the State.*** *Such a public-interest mission could, for example, be reflected* ***through public funding or through provisions in national laws or public contracts.***
    - *Conversely,* ***organisations upon which commercial undertakings have a decisive influence*** ***allowing such undertakings to exercise control*** *because of structural situations, such as through their quality of shareholder or member, which* ***could result in preferential access*** ***to the results of the research, should not be considered research organisations*** ***for the purposes of this Directive.***

European Data Protection Supervisor (EDPS) (Jan. 6, 2020)

가명정보의 입지: 개인정보법

- 비신용정보의 가명조치가 정보주체의 통제권 약화를 위한 근거로 정당한가
  - 가명정보에 대한 광범위한 보호장치 적용 제외: 개인정보법 제28조의7(적용범위) 가명정보는 제20조, 제21조, 제27조, 제34조제1항, 제35조부터 제37조까지, 제39조의3, 제39조의4, 제39조의6부터 제39조의8까지의 규정을 적용하지 아니한다.

<비신용 가명정보에 적용 배제되는 조항>

- 제20조 (정보주체 이외로부터 수집한 개인정보의 **수집 출처 등 고지**)
- 제21조 ([불필요한] 개인정보의 **파기** [의무])
- 제27조 (영업양도 등에 따른 개인정보의 이전 제한)
- 제34조제1항 (개인정보의 **유출 통지** 등)
- 제35조 (개인정보의 **열람**)
- 제36조 (개인정보의 **정정,삭제**)
- 제37조 (개인정보의 **처리정지 등** [요구권])

가명정보의 입지: 개인정보법

- 비신용정보의 가명조치가 정보주체의 통제권 약화를 위한 근거로 정당한가

<비신용 가명정보에 적용 배제되는 조항 (이하 정보통신서비스 제공자 특례) >

- 제39조의3 (개인정보의 수집, 이용 동의 [의무] 등에 대한 특례)
- 제39조의4 (개인정보 유출등의 통지, 신고에 대한 특례)
- 제39조의6 (개인정보의 파기에 대한 특례)
- 제39조의7 (이용자의 [동의철회] 권리 등에 대한 특례)
- 제39조의8 (개인정보 이용내역의 통지)

가명신용정보의 입지: 신용정보법

- 신용정보의 가명조치가 정보주체의 통제권 약화를 위한 근거로 정당한가
  - 가명정보에 대한 광범위한 보호장치 적용 제외: 신용정보법 제40조의3(가명정보에 대한 적용 제외) 가명정보에 관하여는 제32조제7항, 제33조의2, 제35조, 제35조의2, 제35조의3, 제36조, 제36조의2, 제37조, 제38조, 제38조의2, 제38조의3, 제39조 및 제39조의2부터 제39조의4까지의 규정을 적용하지 아니한다.

<가명 신용정보에의 적용 배제 조항>

- 제32조제7항(개인신용정보를 신용정보주체의 **동의 없이** 타인에게 제공할 경우 사전에 신용정보주체에게 **알릴 의무**) *
- 제33조의2(개인신용정보의 **전송요구**) <Right to data portability>
- 제35조(신용정보 **이용 및 제공사실의 조회**) *
- 제35조의2(개인신용평점 하락 가능성 등에 대한 [신용정보주체에게의] **설명의무**)
- 제35조의3([개인신용정보를 신용정보집중기관 등에 제공시] 신용정보제공·이용자의 [신용정보주체에의] **사전통지**)

가명신용정보의 입지: 신용정보법

<가명 신용정보에의 적용 배제 조항>

- 제36조([신용정보주체의 요구가 있는 경우] **상거래 거절 근거 신용정보의 고지 등**)
- 제36조의2([개인인 신용정보주체의] **자동화평가 결과**에 대한 설명 및 이의제기 등) *
- 제37조([개인인 신용정보주체가 갖는] 개인신용정보 **제공 동의 철회권** 등) *
- 제38조([신용정보주체의 신용정보회사 등에 대한] 신용정보의 **열람 및 정정청구** 등) *
- 제38조의2([신용정보주체의] **신용조회사실의 통지** 요청)
- 제38조의3(개인신용정보의 **삭제 요구**)
- 제39조([개인인 신용정보주체의 신용정보 등에 관한] **무료 열람권**) *
- 제39조의2([개인인 신용정보주체의 금융거래 관련] **채권자변동정보**의 열람 등)
- 제39조의3(신용정보주체의 [열람요구등의] **권리행사 방법** 및 절차) *
- 제39조의4([신용정보회사등의] 개인신용정보 **누설통지** 등) *

GDPR상 가명정보의 입지

- Recital (28)
  - The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations.
  - The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

조문번호	조문명	Recital	내용
4	정의	26,28,29	비식별화(비식별조치)의 정의
6	처리의 적법성		목적 제한 테스트에서 새로운 정보 처리목적이 규정과 양립가능한지 여부를 평가할 때 고려할 수 있는 안전항 예로의 비식별화
25	디자인과 디폴트에 의한 정보보호	75,78	정보보호원칙의 집행을 보여주는 조치로서의 비식별화
32	처리의 보안성	85	정보보안조치로서의 비식별화
40	행동규준		행동규준에서 다뤄야 할 사항으로서의 비식별화
89	정보처리 관련 규정의 적용 예외*인 안전항(safeguard) 및 부분수정(derogation)	156	정보최소원칙을 존중하는지를 보여주는 안전항의 사례로서의 비식별화

* 공익, 과학적·역사적 조사 목적 또는 통계 목적을 달성하기 위한 경우를 말한다.

Tarhonen (2016), p.23 [양기진 (2018), 69면에서 재인용]

익명정보 취급의 문제

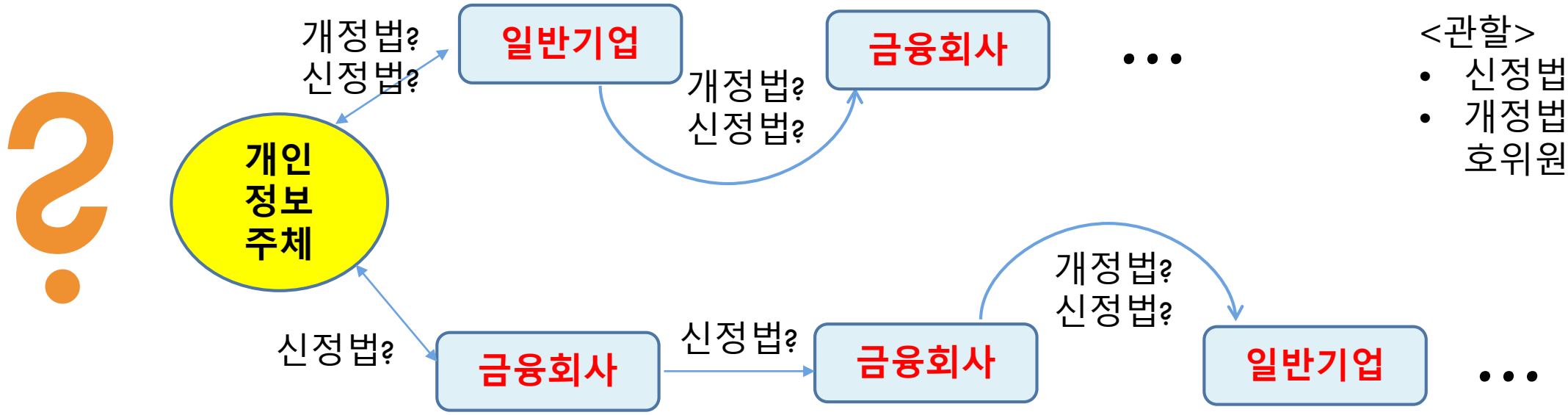
- 신용정보법상 익명정보 취급
  - 익명처리의 적정성에 관한 국가기관의 심사 및 심사후의 법률효과
    - 금융위원회의 적극적 개입(심사 및 법률상 추정력 부여)과 국가배상책임 소지
  - 신용정보법
    - 제40조의2(가명조치·익명조치에 관한 행위규칙) ③ 신용정보회사등은 개인신용정보에 대한 **익명처리가 적정하게 이루어졌는지 여부에 대하여 금융위원회에 그 심사를 요청**할 수 있다.
    - ④ 금융위원회가 제3항의 요청에 따라 심사하여 **적정하게 익명처리가 이루어졌다고 인정한 경우 더 이상 해당 개인인 신용정보주체를 알아볼 수 없는 정보로 추정**한다.
- GDPR
  - 익명정보의 개념을 두면서도 익명정보가 되기 위한 구체적인 조치 수준이 무엇인지에 관하여 **일절 관여하지 않으며** 익명정보 여부의 판정에 관한 **정부당국의 개입 없음**
- 미국
  - 건강정보의 예: 피규제자가 필요조치를 수행하였음을 스스로 증명하여야 함

신용정보법과 개인정보법의 관계

- 신용정보인 개인정보에 대하여 적용되는 법과 감독기관은?
  - 타법 > 신용정보법 > 개인정보법
  - 개인정보 보호위원회의 관할
    - 개인정보법 제7조(개인정보 보호위원회) ① 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리 소속으로 개인정보 보호위원회(이하 "보호위원회"라 한다)를 둔다.
  - 신용정보법
    - 제3조의2(다른 법률과의 관계) ① 신용정보의 이용 및 보호에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.
    - ② 개인정보의 보호에 관하여 이 법에 특별한 규정이 있는 경우를 제외하고는 「개인정보 보호법」에서 정하는 바에 따른다.
  - 개인정보법
    - 제6조(다른 법률과의 관계) 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.

신용정보 범위 설정과 관할/감독상 문제

- 신용정보의 흐름에 따른 관할감독권의 분산
  - 신용정보란 "**금융거래 등 상거래에서** 거래 상대방의 신용을 판단할 때 필요한 정보"
  - 그런데 대부분의 개인정보도 **상거래**에서 발생/처리되는 경향



<관할>
- 신정법: 금융위원회
- 개정법: 개인정보보호위원회

  - 정보의 속성 (흐름)상 감독의 중복, 사각지대의 우려가 없을까?

향후 개선방향

- 신용정보의 개인정보와의 간섭문제
  - 신용정보법을 CB사 등의 감독법으로 하고 개인정보 보호에 관한 사항은 개인정보법에 통합시킬 필요
- 민감정보인 건강정보의 활용/제공 이슈
  - 현출시켜 사회적으로 논의후 적정한 법제화 필요 (가이드라인으로 해결 불가)
- 동의없는 추가처리 범위
  - 원수집 목적과 '양립가능한(compatible)' 경우에 한하여 정보주체의 동의 없는 추가처리를 허용해야
- 가명정보 등에 관한 현재 약화된 자기정보결정권 강화
  - 법 개선하여 가명정보에 관한 개인의 권리를 대폭 부활시켜야
  - 익명정보 여부의 금융위 확인 및 추정효 부여의 삭제
- 과학적/산업적 연구 목적
  - 과학적 연구의 합리적 설정 필요 (가이드라인으로 해결 불가)
  - 산업적 연구를 위한 동의 없는 정보처리는 폐기
    - 정보주체인 개인의 원 수집목적에 반할 소지가 커서, 개인정보주체의 자기결정권 행사를 저해

참고문헌

- 양기진 (2018.10.), “개인정보의 범위에 관한 연구- GDPR의 비식별조치와 약학정보원 사건의 검토”, 선진상사법률연구 통권 제84호, 법무부
- 정희수 (2020.7.24.), “데이터3법 개정이 금융산업에 미치는 영향”, 제휴 보고서, 하나금융연구소 및 BC카드디지털연구소
- 건치 신문 (2020.9.2.), “보건의료 데이터 활용 가이드라인 철회”
- European Data Protection Supervisor (EDPS) (Jan. 6, 2020), “A Preliminary Opinion on data protection and scientific research”, <https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf>
- Tarhonen, Laura (2016). “Pseudonymisation of Personal Data According to the General Data Protection Regulation”, Viestintäoikeuden vuosikirja 2016 <https://www.edilex.fi/viestintaoikeus/18073>
- US HHS.gov., “Summary of the HIPAA Privacy Rule”, <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>
- US HHS.gov., “Summary of the HIPAA Security Rule”, <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>
- US NIH.gov., “Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule”, NIH Publication Number 03-5388, <https://privacyruleandresearch.nih.gov/pdf/HIPAA_Privacy_Rule_Booklet.pdf>

감사합니다