「 '4차 산업혁명'과 정보인권 」 연속토론회

빅데이터 활용과 개인정보 보호, 바람직한 균형은 무엇인가

일 시 | 2017년 7월 26일(수) 오후 2시~4시

장 소 | 국회의원회관 제2세미나실

주 최 |

국회 미래창조과학방송통신위원회
변재일 의원 (더불어민주당, 충북 청주시청원구)
김성수 의원 (더불어민주당, 비례대표)
추혜선 의원 (정의당, 비례대표)
국회 안전행정위원회
진선미 의원 (더불어민주당, 서울 강동구갑)
권은희 의원 (국민의당, 광주 광산구을)
이재정 의원 (더불어민주당, 비례대표)
언론개혁시민연대, 정보인권연구소, 진보네트워크센터, 참여연대, 한국소비자단체협의회, 함께하는시민행동

후 원 | 국가인권위원회

순 서

2:00 ~ 2:05	개회	
2:05 ~ 2:15	인사말	
	사회	김일환 | 성균관대학교 법학전문대학원 교수
2:15 ~ 2:45	발제	이은우 | 정보인권연구소 이사, 변호사
2:45 ~ 3:45	토론	고학수 | 서울대학교 법학전문대학원 교수
		이상윤 | 연구공동체 건강과대안 책임연구위원
		양기철 | 개인정보보호위원회 심의처리과장
		이정현 | 한국인터넷진흥원 정보보호산업분쟁조정위원회 사무국장
3:45 ~ 4:00	전체토론	

20대 국회의 개인정보보호법 개선과제

이은우 | 정보인권연구소 이사, 변호사

I. 빅데이터, 사물인터넷, 개인정보보호법제

1. 빅데이터, 인공지능, 사물인터넷-개인정보보호법제의 개선방향

가. 인공지능, 빅데이터, 로보틱스, 사물인터넷

- 우리나라에서는 4차 산업혁명이라는 용어를 주로 사용하고 있는데, 4차 산업혁명이라는 용어는 보편적인 개념은 아님.
- 미국 정부의 경우 주로 '인공지능과 빅데이터'에 초점을 맞추고 있고, 유럽연합의 경우도 빅데이터, 인공지능, 로보틱스 등이 주로 사용됨.
- 유럽과 미국에서는 인공지능, 로보틱스 등이 가져올 사회의 변화에 대해서 많은 논의가 있는데 반해서 우리나라의 경우는 우리가 당장 선점해야 할 '새로운 미래 먹거리' 정도로 논의가 이루어지고 있는 경향.
- 로보틱스, 사물인터넷과 관련된 이슈는 주로 일자리나 빈부격차, 공정한 경쟁환경 등과 연결.
- 예를 들어 미국의 경우 오바마 행정부의 보고서에서는 노동조합의 역할 강화, 고용 안정, 교육, 조세제도의 대대적 개혁 등이 논의.
- 유럽연합의 경우도 고용 안정, 교육, 조세제도의 개혁 등이 중요한 문제로 제기됨. 유럽연합의 경우 기본소득 보장이 중요한 논의대상으로 제기되었음.

나. 빅데이터, 인공지능, 로보틱스, 사물인터넷과 개인정보의 활용과 보호

– 빅데이터, 인공지능, 로보틱스, 사물인터넷 등과 관련하여 제기되는 주된 이슈는 투명성 부족, 정보의 불균형, 차별 등의 문제. 이 문제를 해결하지 못할 경우 개인정보보호의 핵심원칙이 위험해진다고 봄.

다. 유럽연합 EDPS(European Data Protection Supervisor)의 빅데이터에 대한 의견(2016. 9. 23.)[1)]

– 네 가지 필수 요소에 근거한 책임 있고 지속가능한 빅데이터를 개발해야

(1) 개인정보처리자는 더 투명하게 개인정보를 처리해야 한다 -비밀스런 프로파일링 종결

● 투명성을 제고하기 위해서는 해당 개인에게 명확한 정보 제공
- 개인에 대해 관찰되고 추론된 개인정보가 무엇인지, 어떠한 개인정보가 처리되었는지에 대한 명확한 정보를 제공해야 하며
- 개인정보의 사용 목적과 방법에 대해 보다 확실하게 고지해야

● 알고리즘 포함
- 고지내용에는 목적과 방법에 대한 가정과 예상을 결정하는 알고리즘의 논리(logic)도 포함

● 완벽하게 알 권리
- 관련 정보가 자발적으로 제공되었든, 관찰되거나 추론된 것이든, 또는 공식 출처에서 수집되었든 상관없이 개인은 정보의 출처가 어디며 정보처리자가 해당 정보를 어디서 또 누구로부터 얻게 되었는지에 대해 완벽히 알 권리가 있다.
- 해당 정보와 정보의 출처를 '이해할 수 있는 형식'으로 보다 선제적으로 개인 에게 제공해야 할 필요성이 점점 커짐.

● 영업비밀의 보호
- 원칙적으로 사업상 기밀 또는 영업비밀에 대한 보호가 개인의 프라이버시 및 개인정보보호의 기본권을 우선할 수 없음. 양자는 신중한 균형.
- 공개여부의 흑백논리보다는 평가절차와 공개방법 고려
- 개인이나 대중에게 모든 상세내용을 공개하는 대신 신임 받는 제3자를 평가자로 이용.
- 개인정보보호기관(또는 소비자보호기관, 공정거래당국, 금융 및 보험규제기관 등, 다른 규제

1) 번역 : 개인정보보호위원회(http://www.pipc.go.kr/cmt/not/ntc/selectBoardArticle.do)

기관 등)은 '블랙박스'를 살펴볼 수 있어야 함.
- 투명성에 대한 조문을 더 강화하고, '의사결정 논리'와 정보 및 출처 공개에 관한 조문을 구체화해야

(2) 이용자는 본인의 개인정보가 어떻게 사용되는 지에 대해 높은 수준의 개인정보 통제권

- 이용자 통제권 : 불공정한 편견과 실수에 대한 이의 제기 가능해야 함
- 정보주체의 개인정보 열람권과 정정권이 빅데이터 분석이 발전함에 따라 더욱 중요해짐.
- 개인이 불공정한 편견을 보다 잘 포착하고 예상과 예측(assumptions and predictions)을 결정하기 위한 알고리즘의 논리에서 비롯된 실수를 해결하기 위해서는 강력한 열람권 및 정정권이 전제조건임.
- 자기정보 이전권 : 개인에게 더 많은 통제권을 제공하고, 빅데이터의 혜택을 공유하는 동시에 효율적이고 투명한 개인정보 처리에 대한 인센티브
- 개인이 휴대가능하고 상호호환이 가능하며 기계판독이 가능한(즉, 사용가능하고 재사용가능한) 형태로 본인의 정보에 접근할 수 있도록 허용한다.
- 개인이 본인의 개인정보를 수정, 삭제, 이전하고 다른 방식으로 추가 처리할 수 있도록 허용해야 한다.
- 개인이 제공자를 변경(본인의 사진, 은행 및 피트니스 정보나 이메일을 다른 서비스 제공자에게 이전) 할 수 있도록 허용해야 한다.
- 개인이 본인의 개인정보를 분석하고 유용한 결론을 이끌어내기 위해 제3자를 이용하도록 허용한다.(식단이나 운동습관 변경, 맞춤형 보건서비스 획득, 현명한 투자 결정 내리기, 보다 저렴한 전력공급자로의 변경 등이 있다.)
- 본인의 자기정보이전권이 가능해지면, 기업과 개인은 보다 균형적이고 투명한 방식으로 빅데이터의 혜택을 최대화 할 수 있으며, 정보처리자와 개인 사이의 경제적 불균형 해소에도 도움이 됨.
- 개인에게 통지권, 열람권, 통제권을 제공하기 위해 새롭고 혁신적인 방법이 필요함.

(3) 제품과 서비스에 이용자친화적인 개인정보보호를 설계한다.

- 기능적 분리(functional separation)
- 적절한 익명처리 기법

(4) 정보처리자는 본인업무에 대해 더 책임감을 갖는다.

- 윤리이사회(Ethics boards) 등

Ⅱ. 그 동안의 우리나라의 개인정보의 보호 또는 활용에 대한 논의의 흐름

1. 우리나라의 4차 산업혁명과 개인정보보호

가. 일자리 창출

- 일자리 창출을 위해 개인정보 보호 완화를 해야 하는가?
- 빅데이터 산업의 육성을 위해 개인정보 보호 완화해야 하는가? 빅데이터 산업이 개인정보 보호 완화로 육성되는가?
- 오히려 개인정보 보호 완화는 불공정경쟁을 촉진하고, 대기업 집중을 초래함.

나. 빅데이터 산업 육성과 첨단 산업 육성과 개인정보의 활용

- 4차 산업혁명에 대응하는 것은 첨단 IT 기업의 육성인가?
- 빅데이터 산업 육성이 개인정보 보호 완화와 어떤 관계가 있는가?

다. 균형 잡힌 시각이 필요함

- 우리나라에서 4차 산업혁명과 개인정보보호 이슈는 주로 활용, 규제 완화론과 함께 논의.

2. 규제완화론의 흐름

가. ‘프라이버시 정책연구 포럼’(2013)

- 다양한 형태의 규제완화론의 흐름
- 한국인터넷기업협회의 후원으로 정책연구 활동을 펼친 프라이버시 정책연구 포럼(의장 이인호)의 ‘개인정보보호법제 개선을 위한 정책연구보고서’(2013)는 대체로 규제완화론의 흐름을 반영
- 방송통신위원회의 빅데이터 개인정보보호 가이드라인
- 비식별조치 가이드라인

나. 빅데이터 가이드라인과 비식별조치 가이드라인 : 성급한 ‘비식별화’

- 2013년도부터 시작된 방송통신위원회에서 제정한 ‘빅데이터 개인정보보호 가이드라인’
- ‘비식별조치 가이드라인’
- 익명화를 ‘비실명개인정보’ 등의 개념을 사용하여 개인정보보호법의 적용범위를 축소하려는 시도, 동의 규정을 완화해야 한다는 시도가 대표적이다.

다. 규제프리존법과 규제완화론

- 박근혜 정부의 창조경제론과 창조경제혁신센터, 창조경제혁신센터에 참여하는 대기업들이 중심이 되어 추진된 규제프리존은 규제의 기본 틀을 변경하고자 하는 내용이었다.

- 개인정보와 관련해서는

라. 개인정보보호법과 맞지 않는 빅데이터 관련 가이드라인이 병존함

3. 보호강화론의 흐름

가. 시민사회단체의 활동

- 프로파일링 규제, 투명성 강화, 개인정보영향평가 확대, 권리 구제제도 강화, 감독기구 독립성과 권한 강화, 콘트롤타워 구축 등
- 개별법의 개정 활동

나. 국회의 대응

- 법률안 수로는 개인정보 강화 입법이 많음.
- 크게 실효성이 없는 임시방편적인 입법
- 대규모 개인정보유출사태가 발생하면처처벌규정을 강화한다거나, 새로운 제도를 도입하는 것들이 그것이었다.

4. 최근 개인정보보호법 개정에 대한 의견이 다수 제시되고 있음

가. 다수의 의견 제시

- 개인정보보호위원회 연구용역

- 방송통신위원회 연구용역
- 시민단체들의 주장

나. 전면적인 문제제기와 전면 개정에 준하는 개인정보보호법제의 개선이 필요함

- 지금까지 제기된 개인정보보호법의 문제점에 대한 허심탄회한 토론이 필요함.
- 지나치게 엄격하다는 주장 vs 규정이 미비하다는 주장
- 규제가 너무 강하다는 주장 vs 규제 시스템이 작동하고 있지 않다는 주장
- 해외 사례의 아전인수식 주장
  - 비식별화, 비식별 조치
  - 미국의 개인정보 관련 집행
  - 유럽연합의 개인정보 보호법제
  - 유럽연합의 GDPR

Ⅲ. 지금까지 20대 국회에 제출된 개인정보 관련 법률안의 검토 및 평가

1. 개인정보와 관련된 주요 법률안의 검토

- 의안의 주요 요지에 '개인정보'가 포함된 법률안은 20대 국회에서는 166건(19대 포함시 583건)

• 개인정보 관련 주요 4법(개인정보보호법, 정보통신망법, 신용정보법, 위치정보법)

• 빅데이터산업발전법 등 개인정보와 관련된 새로운 법률안.

- 20대 국회에 제출된 법률개정안의 내용을 분석해 보면

• 비식별개인정보와 관련한 법률 개정안 또는 법률안이 5건임(비식별개인정보에 대한 규정을 담은 개인정보보호법안은 개인정보의 보호범위를 대폭 축소하는 것임.)

• 그 외에는 대부분이 개인정보보호에 치중하고 있는 법률들임. 그러나 그 내용은 부분적이거나, 특별한 사건에 대응한 단편적인 내용임.

2. 개인정보보호법 개정안의 검토

가. '비식별조치 개인정보', '비식별개인정보' 등의 내용을 포함한 법률안

- 비식별조치에 대한 규정을 담은 법률 개정안은 개인정보보호법, 정보통신망법, 신용정보법에 모두 제출되어 있음. 규제프리존법, 빅데이터산업발전법에도 포함되어 있음.

• 개인정보보호법(송희경, 김병기), 정보통신망법(이은권, 윤영석), 신용정보법(추경호)이 제안되어 있고, 규제프리존법, 빅데이터산업발전법.

- 예를 들어 송희경 의원은 제22조의2(비식별정보의 이용·제공 등)이라는 제호 아래 아래의 규정을 신설하는 법안을 제출함.

제22조의2(비식별정보의 이용·제공 등) ① 개인정보처리자는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 없는 경우 데이터 값 삭제, 가명처리, 총계처리, 범주화 등 개인정보를 전부 또는 일부 삭제하거나 대체하여 다른 정보와 쉽게 결합하여도 개인을 알아볼 수 없도록 조치(이하 “비식별조치”라 한다)하여 생성한 정보(이하 “비식별정보”라 한다)를 정보주체의 동의 없이 개인정보의 목적 외의 용도로 이용하거나 제3자에게 제공할 수 있다.
② 개인정보처리자는 비식별정보를 처리하는 과정에서 개인정보를 생성하기 위한 행위를 하여서는 아니 된다. 다만, 부득이하게 개인정보가 생성되는 경우에는 대통령령으로 정하는 바에 따라 지체 없이 회수·파기하거나 추가적인 비식별조치를 하여야 한다.
③ 개인정보처리자는 비식별정보를 처리하는 경우에는 그 비식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 조치를 하여야 한다.
④ 개인정보처리자는 비식별조치의 적정성을 평가하기 위하여 대통령령으로 정하는 바에 따라 제31조에 따른 개인정보 보호책임자를 포함한 평가단을 구성·운영하여야 한다.

- 이는 ‘비식별화, 비식별개인정보’ 등의 용어를 통해서 사실상 개인정보보호법의 적용범위를 대폭 제한하려는 것임.

의안명	주요 내용
송희경의원 등 11인	비식별조치의 정의와 비식별조치된 정보의 관리 방안을 법률에 규정하고, 개인정보 보호 및 이용 정책의 통일적·독립적 수행을 위해 개인정보 보호위원회를 중앙행정기관으로 격상시키려는 것
김병기의원 등 14인	현행법상 비식별조치와 관련된 내용을 보다 구체화하고, 비식별조치를 통하여 생성된 비식별정보를 처리하는 과정에서의 안전성 확보 의무 및 위반 시 처벌 조항 등을 신설함으로써, 정부의 가이드라인이 아닌 법률에 비식별조치를 규정하여 개인정보 보호를 강화하려는 것임

나. 개인정보 이용제한, 개인정보 동의 명확화, 기타

- 개인정보의 이용을 제한하는 내용의 법률로는 개인정보 매매금지(윤영석, 홍의락, 김정재), 개인정보 제공동의 요건 명확화(정재호, 심재권), 수사기관의 민감정보 열람시 영장주의(강병원) 등이 있음.

의안명	주요 내용
윤영석의원 등 10인	정보주체가 개인정보의 제3자 제공에 동의하였다 하더라도 이를 매매하여 기업이 이익을 취하는 것을 금지하고, 이와 관련한 처벌조항을 마련
정재호의원 등 10인	개인정보 수집·제공 동의서에 대한 기준 마련의 근거를 법에 상향하여 규정하고자 함
심재권의원 등 17인	개인정보처리자가 서면 등으로 정보주체의 동의를 받을 때 중요한 내용은 부호, 색채 및 굵고 큰 문자 등으로 명확히 표시하여 알아보기 쉽게 표시하도록 명시함으로써, 국민의 헌법상 인정되는 기본권 중 하나인 개인정보 자기결정권을 더욱 보호하고자 함
홍의락의원 등 10인	개인정보처리자가 영리목적으로 개인정보를 제3자에게 제공하지 못하도록 규정하고, 이를 위반할 경우 처벌근거를 마련함으로써 정보주체의 자기결정권을 보호하려는 것임
김정재의원 등 11인	정보주체가 개인정보의 제3자 제공에 동의하였다 하더라도 이를 매매하여 기업이 이익을 취하는 것을 금지하고, 이와 관련한 처벌조항을 마련하고자 함
정재호의원 등 10인	개인정보 수집·제공 동의서에 대한 기준 마련의 근거를 법에 상향하여 규정하고자 함
강병원의원 등 13인	수사기관 등이 건강 등 민감정보를 열람하고자 할 때에는 통신사실이나 금융거래정보와 같이 법원의 영장을 발부받도록 하는 절차를 추가하고, 열람한 이후에는 개인에게 통지하도록 의무를 부과함으로써 개인의 자기정보결정권을 두텁게 보호하려는 것임

다. 피해배상 강화, 개인정보 감독기구 권한 강화 등

- 개인정보보호위원회 위상 강화(송희경, 소병훈), 분쟁조정제도 보완(김도읍), 피해배상제도 보완(이학영, 이효상 등).

의안명	주요 내용
황주홍의원 등 10인	행정자치부장관이 개인정보관리 수준 및 실태파악 등을 위한 조사를 실시한 경우 국회의 소관 상임위원회에 보고하도록 함
송희경의원 등 11인	비식별조치의 정의와 비식별조치된 정보의 관리 방안을 법률에 규정하고, 개인정보 보호 및 이용 정책의 통일적·독립적 수행을 위해 개인정보 보호위원회를 중앙행정기관으로 격상시키려는 것
소병훈의원 등 10인	개인정보 보호위원회의 위상을 중앙행정기관으로 격상하여 개인정보 관련 정책을 총괄하도록 하고, 개인정보 침해에 대한 효율적인 권리

	구제를 위해 직권조사권, 시정명령권, 고발 및 징계권고권 등의 권한을 부여함으로써, 효율적이고 통일적인 개인정보 보호 정책을 추진할 수 있도록 하려는 것임
김도읍의원 등 10인	분쟁조정의 처리기간 연장 사유를 '부득이한 사정'에서 '정당한 사유'로 변경함으로써 분쟁조정제도의 명확성과 신속성을 확보하려는 것임
이학영의원 등 14인	집단소송 및 배상명령제도를 도입하여 개인정보의 불법 유출 가능성을 억제하고 피해자들에 대한 구제를 보다 효율적으로 하려는 것
강효상의원 등 10인	현행법에 생체정보의 정의 및 처리에 관한 규정을 마련함으로써 생체정보의 보호를 통해 개인의 자유와 권리 보호에 이바지하고자 함
민경욱의원 등 11인	생체정보의 정의 및 처리에 관련된 사항을 규정함으로써 생체정보 보호의 법적 근거를 마련하고자 함.

3. 개인정보와 관련된 정보통신망법 개정안

가. 비식별정보

의안명	주요 내용
이은권의원 등 32인	특정한 개인을 알아볼 수 없도록 개인정보를 가공처리하는 비식별조치를 규정하고, 정보통신서비스 제공자등이 비식별화된 정보를 처리하는 과정에서 개인정보가 발생하는 경우에는 이를 지체 없이 파기하거나 다시 비식별화하는 의무를 부과함으로써 개인정보를 보다 안전하게 보호하려는 것임
윤영석의원 등 11인	특정한 개인을 알아볼 수 없도록 개인정보를 가공처리하는 비식별조치를 규정하고, 정보통신서비스 제공자등이 비식별화된 정보를 처리하는 과정에서 개인정보가 발생하는 경우에는 이를 지체 없이 파기하거나 다시 비식별화하는 의무를 부과함으로써 개인정보를 보다 안전하게 보호하려는 것임

나. 이용자 권리 보장 등

의안명	주요 내용
이재정의원 등 12인	일정 규모 이상의 정보통신망서비스 제공자 등에 대하여 '개인정보보호 관리체계 인증제도'를 의무화하여 기업의 개인정보보호 관리수준을 제고하고 국민의 개인정보 보호수준을 보다 강화하고자 함
정부	정보통신서비스를 이용하는 자의 개인정보를 보호하기 위하여 이용자는 정보통신서비스 제공자 등에 대하여 언제든지 개인정보 처리의

	정지를 요구할 수 있는 권리를 행사할 수 있도록 하고, 정보통신서비스 제공자 등이 이용자의 개인정보를 국외에 제공하는 경우 이용자의 권리 침해를 예방하기 위하여 국외이전 중단 명령 제도를 도입하는 등 현행 제도의 운영상 나타난 일부 미비점을 개선·보완하려는 것임
박대출의원 등 10인	매출액 또는 일평균 이용자 수를 기준으로 일정 규모를 초과하는 정보통신서비스 제공자 등의 경우에는 개인정보보호 관리체계 인증을 의무적으로 획득하게 하고, 연 1회 이상에서 연 2회 이상으로 사후관리실시를 강화함으로써 정보통신서비스 제공자의 체계적인 개인정보보호 활동을 촉진하고, 국민의 개인정보를 더욱 강하게 보호하려는 것
신경민의원 등 13인	스마트폰 어플리케이션(이하 '앱')이 과도한 접근권한을 요구하고 있는 경우 사후에라도 이를 시정할 수 있도록 하기 위해 방송통신위원회가 이를 심사하고 시정조치를 명할 수 있게끔 함으로써, 이용자의 개인정보를 보호하고 범죄에 악용될 수 있는 위험성을 최소화 시키고자 하려는 것임
황주홍의원 등 11인	매출액 또는 일평균 이용자 수를 기준으로 일정 규모를 초과하는 정보통신서비스 제공자 등의 경우에는 개인정보보호 관리체계 인증을 의무적으로 획득하도록 함으로써 정보통신서비스 제공자의 체계적인 개인정보보호 활동을 촉진하고, 국민의 개인정보를 더욱 강하게 보호하려는 것임
황주홍의원 등 12인	정보통신서비스 제공자 단체 등이 이용자의 개인정보를 보호하기 위한 행동강령을 제정하여 시행할 수 있도록 함으로써 개인정보보호에 관한 자율 규제를 강화하고, 관련 사업자들의 개인정보 취급에 관한 책임성을 강화하려는 것
오세정의원 등 22인	현행법 제4장의 개인정보의 보호에 관하여 현행법과 「개인정보 보호법」의 적용이 경합하는 경우 현행법을 우선하여 적용하도록 함으로써 개별법 사이에 모순이 발생하는 것을 방지하고, 불합리한 상황을 해소하려는 것
강효상의원 등 11인	현행법의 정의조항에 생체정보에 관한 내용을 추가하고, 생체정보의 보관 및 파기 등에 필요한 사항을 규정함으로써 개인정보 자기결정권을 보다 두텁게 보장하고자 함

다. 피해배상 강화 등

의안명	주요 내용
고용진의원 등 19인	대통령령으로 정하는 일정 규모 이상의 정보통신서비스 제공자 등이

	고의 또는 과실로 이용자의 손해를 일으킨 경우, 그 손해의 배상을 보장하기 위하여 배상책임보험에 가입 또는 금융기관에 자산 예탁을 의무화하는 동시에 이를 이행하지 않을 시 2천만원 이하의 과태료를 부과하도록 하려는 것임. 또한 집적된 정보통신시설의 장애로 발생한 피해 보상을 의무화하기 위해 과태료 수준을 2천만원 이하로 강화하려는 것임
백재현의원 등 10인	중대한 과실로 인한 개인정보의 분실·도난은 현행과 같이 손해액의 3배의 범위 내에서 손해배상을 하되, 고의로 개인정보가 분실·도난된 경우에는 손해배상을 손해액의 3배 이상으로 함으로써 개인정보 유출피해를 실효적으로 방지하려는 것임

4. 신용정보의 이용 및 보호에 관한 법률 개정안[2)]

의안명	주요 내용
박경미의원 등 13인	금융 관련 범죄혐의가 있다고 인정될 만한 상당한 이유가 있는 경우 당사자의 동의 없이 신용정보회사, 신용정보집중기관 및 신용정보제공·이용자에게 수집·제공할 수 있도록 함으로써 위법한 금융 관련 피해로부터 국민의 재산과 생활을 보호하고 보다 건전한 신용질서를 확립하고자 함
김영주의원 등 12인	신용정보회사가 금융소비자의 불이익정보를 최장 5년까지 관리 및 등록할 수 기간을 3년으로 단축하여 금융소비자에게 건전한 경제활동의 기회를 주고자 함
박선숙의원 등 17인	정보통신 기술의 발전으로 중요성이 높아진 신용정보에 대한 정의를 대통령령에 위임하지 않고 법에서 규정하여, 하위법령의 개정을 통한 정보 보호범위의 축소를 방지하고 국민의 기본권 보호를 강화하려는 것임
추경호의원 등 14인	개인신용정보의 정의에 비식별화된 경우에 해당 정보를 활용할 수 있도록 하는 단서를 명시적으로 규정

2) 위치정보의 보호 및 이용 등에 관한 법률 개정안 중 송희경 의원 등 11인의 개정안은사물위치정보를 수집·이용·제공할 경우 그 소유자의 사전동의 없이도 처리될 수 있도록 허용하는 내용임.

5. 빅데이터 이용진흥법, 지능정보사회기본 등 개별법률을 통한 법령 제정과 개정시도

- 개별법률을 통한 법령의 제, 개정 시도 : 개인정보보호법을 회피하려는 법령 개정의 방법, 개별 법률에서 위원회 등을 통해서 법률 개정, 제도개선 등을 추진하는 방법.
  - 빅데이터의 이용 및 산업진흥에 관한 법률안(배덕광 의원)은 비식별 개인정보에 대한 규정을 담고 있음[3].
  - 지능정보사회기본법안은 '지능정보기술 관련 법·제도 개선에 관한 사항' '지능정보기술 관련 법령 등 규제 개선에 관한 사항, 소관 법령 및 위원회규칙의 제정·개정 및 폐지에 관한 사항'을 소관사무로 하는 위원회를 구성하도록 하고, 정부는 지능정보기술 관련 법령 등의 규제를 일원화·체계화·간소화하기 위하여 지속적으로 노력하여야 한다는 규정과, 정부는 법령 등 규제를 정비함에 있어 '민관협력포럼'의 의견을 들어야 한다는

---

3) 이 법안의 제안이유에서 '빅데이터산업은 사물인터넷·클라우드 컴퓨팅 산업 등과 함께 정보통신산업의 성장을 이끌 한 축으로서 성장 가능성이 높으나, 국내에서는 개인정보 보호와 관련된 규제의 경직성으로 인하여 많은 기업들이 빅데이터 사업에 적극적으로 나서지 못하는 상황'이라는 진단 아래, '빅데이터 등 정보통신산업에서의 개인정보 활용 형태는 기존의 '개인정보처리자-정보주체'라는 양자적 구조의 범위를 이미 넘어선 상태인 반면, 개인정보에 관한 현행법은 이와 관련된 규정이 마련되어 있지 않음. 이에 빅데이터산업의 가치 제고를 위하여 현행 개인정보 보호 법제에서 공백으로 남겨두고 있는 비식별화된 개인정보의 취급에 관한 사항을 규정함으로써 법률의 명확성을 제고하는 한편, 신성장 산업인 빅데이터 산업의 진흥과 그 이용의 활성화에 관한 사항을 규정하여 개인정보의 침해를 방지하고 국민경제의 발전에 이바지하려는 것임'이라고 밝히고 있다.

규정을 두는 등의 시도를 함.

• 규제프리존법안도 비식별 개인정보에 대한 규정 등을 담고 있음.

- 이런 방법들은 바람직한 방법으로 보기 어려움.

6. 전체적인 평가

- 현재의 상황에 맞는 법률개정안이 제시되고 있지 않은 상태임.
- 정부나 국회는 아직 빅데이터, 인공지능, 사물인터넷 등의 활용 강화에 따른 개인정보와 관련한 문제의식이 정리되지 않은 상태임.
- 정부와 국회는 빅데이터, 인공지능, 사물인터넷 등의 활용 강화에 따른 개인정보와 관련한 문제의식을 정리해야 할 것임.
- 20대 국회에서 법률개정안을 마련할 필요가 있음.

IV. 최근의 논의 및 그에 대한 평가

1. 학회, 시민단체 등의 법률 개정에 대한 의견

가. 개인정보보호위원회의 연구 용역 결과

(1) 경위

- 개인정보보호위원회가 2016년도 개인정보보호위원회 정책연구용역으로 고려대학교 산학협력단을 통해 수행하도록 한 연구용역(EU 개인정보보호

법제(GDPR) 분석 및 개인정보보호법제 개선 입법수요 연구, 이하 '입법수요 연구')는 다음과 같이 현행 개인정보보호법의 개정방안을 제시[4].

(2) 입법수요 연구 결과의 주요 제안 사항

- 투명성 원칙 명시
- 아동 보호
  - SNS와 같은 인터넷서비스 이용 과정에서 아동에 대한 보호의 필요성을 특별히 강조, 이와 관련된 규정 마련할 필요.
- 개인정보주체의 권리를 새롭게 반영하거나, 기존의 권리를 보다 상세하게 규율할 필요.
  - 개인정보보호법이 규율하지 않고 있는 GDPR의 규정으로 잊혀질 권리, 자기정보 이전에 관한 권리, 프로파일링을 비롯한 개인에 관한 자동의사결정(Automated individual decision making)에 종속되지 않을 권리 등을 들고 있음.
  - 연구는 특히 '자기정보 이전에 관한 권리'는 빅데이터 시대에 정보주체의 자기정보에 대한 결정권을 강화하는 한편 스타트업기업과 소규모업체에게는 디지털시장에서 대기업에게 선점된 개인 정보시장(data market)에 접근할 수 있는 기회를 제공함으로써 기업 간 경쟁 과 혁신을 증진시킬 것으로 기대할 수 있다고 의의를 설명함.
- 열람권, 삭제권 및 정정권

4) 입법수요 연구 27페이지~ 28페이지

• GDPR의 유사 규정을 참고하여 보다 상세하게 규율될 필요가 있다고 봄.

- 사전평가제 도입

• GDPR은 사전평가의 결과, 해당 개인정보의 처리가 위험하다고 판단되는 경우, 사전협의 과정에서 감독당국이 처리의 금지를 포함하여 구속력 있는 제재를 가할 수 있도록 규정하고 있으므로, 개인정보보호법도 개인정보침해의 위험성을 사전에 평가하고 개인정보침해 위험을 사전에 저감할 수 있는 관련 규정을 마련할 것 제안

- 업계의 행동강령

• 개인정보처리자의 개인정보처리 방침에 관한 행동강령의 자체적인 제정을 법률로서 권고

- 개인정보 국외이전 규율

• 선언적 조항을 구체적이고 세부적인 규정으로

- 감독당국의 독립성과 권한 부여

- 가명처리 규정

• 정의조항에서 '가명처리'의 개념 을 정의,

• 가명 처리 관련 규정으로 재정비

- 통계, 연구 목적 활용

• 개인정보보호법 제18조 2항 4호를 '. 통계 및 연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 가명처리하여 이용·제공하는 경우'로 개정 제안

- 프로파일링 관련 규정

• GDPR의 프로파일링 규정을 참조하여 법률에 프로파일링에 대한 별도

의 개념을 규정할 필요

• 개인정보처리자가 프로파일링시 프로파일링의 존재여부, 수반된 논리구조에 관한 유의미한 정보, 프로파일링 처리의 중요 성 및 예상되는 결과 등을 정보주체에게 고지하도록 규정할 필요.

• 정보주체가 프로파일링을 포함하여 오로지 자동화된 방식에 의한 개인정보 처리에 따른 의사결정이 자신에 대한 법적 효력을 초래하거나 이에 상응하는 정도로 중대한 영향을 미치는 경우, 그러한 의사결정에 구속되지 않을 권리를 명시[5)]

- 개인정보보호법 제1조 목적 규정

• 개인정보의 활용이라는 목적을 명시[6)]

- 미국 및 일본의 법제를 반영한다면

• 정의조항에서 미국의 비식별정보(de-identified data) 또는 일본의 익명가공정보와 같이 비식별 조치가 취해진 정보를 별도로 정의

• 상기 정의된 비식별 정보는 개인정보에 해당하지 않는다는 사실을 명시하여, 해당 정보를 개인정보보호법의 적용 범위에서 배제

• 비식별 정보의 재식별화를 금지하는 관련 규정

• 공익을 위한 기록보존, 과학 및 역사 연구, 통계의 목적으로 개인정보 활용의 범위를 제한하고 있는 GDPR과 달리 비식별 처리 정보의 활용 범위가 제한되지 않게 된다고 주장[7)].

---

5) 입법수요 연구 64페이지

6) 입법수요 연구 55~56페이지

7) 입법수요 연구 56페이지

(3) 검토

- 종합적인 법률 개선 사항을 제시한 것은 매우 긍정적임.
- 특히, 투명성의 원칙, 프로파일링에 대한 규율이 필요하다는 점은 중요한 지적임.
- 개인정보 이전할 권리
- 개인정보영향평가제도 등에 대해서도 구체적인 입법 개선이 필요함.
- 개인정보보호 감독기구나 구제기구도 한꺼번에 정비되어야 함.

나. 방송통신위원회의 연구 용역 결과

(1) 경위

- 방송통신위원회가 2016년도 방송통신위원회 방송통신발전기금 방송통신융합 정책연구사업으로 진행하여 가천대학교 산학협력단(연구원 최경진/고학수/이창범/안정민)이 수행한 GDPR 등 EU와 우리나라의 온라인상 개인정보보호 법제 비교 연구(2016년 11월, 이하 '법제 비교 연구')는 아래와 같이 정보통신망법 개정안을 제안.

(2) 법제 비교 연구의 제안사항

- 개인정보 목적 변경
  - 정보통신서비스 제공자는 ① 개인정보의 수집·이용 목적, ② 수집하는 개인정보의 항목, ③ 개인정보의 보유·이용 기간 중 어느 하나라도 변 경이 있으면 원칙적으로 변경동의를 받아야 하지만, 개인정보의 수집· 이용

목적과 관련하여 기존 서비스와 합리적인 관련성이 있는 기능 추가 등 서비스 개선은 목적 변경으로 보지 않도록 개정할 필요[8].

- 개인정보처리의 질

  • GDPR은 개인정보처리자가 정보주체의 요구에 따라 개인정보를 정정, 삭제, 처리제한 등을 한 경우에는 개인정보를 제공받은 각각의 수령인에게 개인정보의 정정, 삭제, 처리제한에 관한 사실을 통지하도록 의무를 부과하고 있는 바, 우리나라에서도 정보주체가 자신의 권리를 쉽게 행사할 수 있도록 도입 가능성을 검토해 볼 필요. 다만, 정정·삭 제·처리정지 등의 통보의무는 개인정보처리자들에게 또다른 비용 발생 요인이 되고, 개인정보처리자로부터 통보를 받은 수령자들이 정정·삭제를 이행한다는 보장도 없으므로 제도의 실효성에 대한 면밀한 검토가 필요[9].

- 고지 사항

  • 국외이전과 관련한 사항(적정성 결정 유무, 보호수단 유무, 보호수단의 입수 방법 및 장소, 적정성 결정을 받지 않은 제3국으로 이전시 구체적 위험 등)을 고지사항에 추가

  • 자동화된 의사 결정에 관한 사항(자동화된 의사결정의 존재 사실, 관련된 로직(logic), 정보주체에게 미칠 유의성 및 예상결과 등)도 고지사항에 추가

  • 정보주체의 알권리 강화와 선택권 보장을 위해 적극적인 검토가 필요

  • 개인정보 제3자 제공시 반드시 수령인의 이름을 일일이 나열하지 않고

---

8) 법제 비교 연구 106 ~ 107페이지

9) 법제 비교 연구 116페이지

수령인의 범주를 알리는 방법도 허용, 개인정보의 보관기간을 고지하는 경우에도 보존기간을 알리는 것이 불가능한 경우에는 보관기간을 결정하는데 사용되는 기준을 알리는 것도 허용하는바 우리도 법개정 필요[10].

- 안전성의 원칙
  - 우리나라는 기술적·관리적 보호조치의 수준을 획일적으로 규정하고 있지만, GDPR은 보호 조치의 수준을 위험에 비례해서 개인정보처리자 또는 수탁처리자가 자율적으로 정하도록 규정. 즉 개인정보처 리자와 수탁처리자는 최신기술 및 이행비용뿐만 아니라, 처리의 성격· 범위·관계(상황)·목적, 개인의 권리와 자유에 미치는 위험의 가능성 및 심각성까지 고려해서 그 위험에 적합한 정도의 보안수준을 구축할 것을 요구
  - 개인정보처리자 또는 수탁처리자가 공인된 행동규칙(제40조) 또는 공인된 인증메커니즘을 준수한 경우에는 이를 안전성 조치의무를 이행한 증거로 이용할 수 있게 하고 있음. 우리나라도 개인정보처리자등이 개인정보보호 관련 인증을 취득한 경우에는 보호조치 의무를 다한 것으로 간주내지 추정하거나 최소한 개인정보처리자등이 이를 의무이행의 증거로 활용할 수 있도록 법적 근거를 마련하는 것이 바람직하다고 주장[11].
- 국외이전과 재이전
  - 개인정보 보호의 국제적인 수준을 담보하는 구체적인 기준 마련해야 함
  - GDPR이 제시하는 개인정보 보호 메커니즘을 수용할 필요[12][13]

---

10) 법제 비교 138 ~ 139페이지

11) 법제 비교 연구 155페이지

12) 법제 비교 연구 159 페이지

13) 법제 비교 연구 166 ~ 167페이지

- 프로파일링에 대한 규정

  • GDPR과 같이 프로파일링을 명시적으로 제시하고, 개별적으로 규정해야 하는 사회적 요구가 점차 높아질 가능성이 높다.

  • 그래서 아직 프로파일링에 대한 구체적인 규정을 가지고 있지 않은 현재 한국의 개인정보에 대한 규제 체제에 이런 GDPR 의 규정 태도는 어느 정도의 시사점을 가지고 있다[14].

- 비식별화 가명화

  • GDPR의 가명화와 같이 개인정보의 보호에 대한 구체적인 기술적 관리 조치를 법규정 에 명시하는 방식은 개인정보가 보호되면서 활용되는 실질적인 방식을 제시한다는 관점에서 한국의 법제에서도 참조할만하다고 함[15].

(3) 법제 비교 연구의 법률개정안

- 국외이전에 대한 규정
- 개인정보 처리기준 완화

  • 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우 →이용자와 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우

- 개인정보 처리시 동의를 받을 사항 축소

---

14) 법제 비교 연구 173 ~ 174 페이지

15) 법제 비교 연구 183 페이지

(4) 평가

- GDPR의 다수의 규정을 균형 있게 검토, 반영했다고 보기 어려움.
- 특히 투명성, 개인정보주체의 통제권, 개인정보 이전권, 개인정보영향평가 등에 대해서 그 의의와 도입 필요성 등을 간과하고 있음.
- 법률개정이 필요하다고 한 것이 GDPR의 규정과 배치되는 것도 있음
  • GDPR은 공인된 행동규칙(제40조) 또는 공인된 인증메커니즘을 준수한 경우 보호조치를 다한 증거로 활용할 수 있다고 하고 있는데, '준수'는 단순히 '인증'을 받은 것이 아니라, 기준을 준수하는 것임. 따라서 이 규정을 두고 우리나라도 개인정보처리자등이 개인정보보호 관련 인증을 취득한 경우에는 보호조치 의무를 다한 것으로 간주 내지 추정하거나 최소한 개인정보처리자등이 이를 의무이행의 증거로 활용할 수 있도록 법적 근거를 마련하는 것이 바람직하다고 하는 것은 부적절한 주장임.
- 투명성과 관련하여
  • 프로파일링에 대한 고지 등 고지사항의 추가는 입법 필요성을 검토할 필요가 있다고 하고, 고지사항 단순화(제3자 제공의 상대방을 범주로 표시, 보존 기간 규정)하는 내용만 개정안 작성
- 현행 개인정보보호법의 규정을 완화하는 내용의 법률 개정만을 제안함
  • 개인정보 처리 목적과 관련하여 연구는 '합리적인 관련성, 기능 추가, 서비스 개선'을 목적 변경으로 보지 않는 개정을 제안하였으나, 두 서비스 사이의 목적의 양립가능성 판단 기준이 다양할 수 있음.
  • 개인정보 주체의 알 권리나 투명성 강화를 위해 필요한 수 많은 규정에도 불구하고, 이 규정을 개정 필요사항으로 제안한 것은 균형 잡힌 시각으로 보기 어려움.

2. 방송통신위원회의 대응 입법

가. 정보통신망법 개정안(2017년 3월 8일 제출)

- 아래와 같이 개인정보 수집, 이용 동의 요건을 완화하는 것만을 개정안으로 냄.

현 행	개 정 안
제22조(개인정보의 수집 · 이용 동의 등) ① (생 략)	제22조(개인정보의 수집 · 이용 동의 등) ① (현행과 같음)
② 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 제1항에 따른 동의 없이 이용자의 개인정보를 수집 · 이용할 수 있다.	② ---------- ---------- .
1. 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적 · 기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우	1. 이용자와의 정보통신서비스의 제공에 관한 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
2. (생 략)	2. (현행과 같음)
〈신 설〉	3. 이용자 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 이용자 또는 제3자의 급박한 생명, 신체 또는 재산상의 이익을 위하여 필요하다고 인정되는 경우
3. (생 략)	4. (현행 제3호와 같음)
〈신 설〉	③ 제1항 각 호 외의 부분 후단의 경우에 종전의 정보통신서비스와 밀접한 관련성이 있다고 합리적으로 인정되는 범위에서 기능이 추가되는 정보통신서비스 개선은 제1항제1호에 따른 개인정보의 수집 · 이용 목적의 변경으로 보지 아니한다.
제24조의2(개인정보의 제공 동의 등) ① 정보통신서비스 제공자는 이용자의 개인정보를 제3자에게 제공하려면	제24조의2(개인정보의 제공 동의 등) ① ---------- - 제22조제2항제2호부터 제4호까지의

제22조제2항제2호 및 제3호에 해당하는 경우 외에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.	규정----------.
1. & 4. (생 략)	1. & 4. (현행과 같음)
〈신 설〉	5. 개인정보를 유상으로 판매하는 사실(개인정보를 판매하는 경우에만 해당한다)
② (생 략)	② (현행과 같음)
제25조(개인정보의 처리위탁) ① 정보통신서비스 제공자와 그로부터 제24조의2제1항에 따라 이용자의 개인정보를 제공받은 자(이하 &정보통신서비스 제공자등&이라 한다)는 제3자에게 이용자의 개인정보를 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(이하 &처리&라 한다)를 할 수 있도록 업무를 위탁(이하 &개인정보 처리위탁&이라 한다)하는 경우에는 다음 각 호의 사항 모두를 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.	제25조(개인정보의 처리위탁) ①---------- ---------- ---------- ---------- ---------- ---------- ---------- 제27조의2에 따른 개인정보 처리방침에 정하여 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알려야 --. -----.
1. · 2. (생 략)	1. · 2. (현행과 같음)
② 정보통신서비스 제공자등은 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 제1항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁에 따른 제1항의 고지절차와 동의절차를 거치지 아니할 수 있다. 제1항 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.	② 제1항에도 불구하고 정보통신서비스 제공자등은 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하기 위하여 이용자의 개인정보 처리위탁을 하는 경우 제1항 각 호의 사항 모두를 제27조의2에 따른 개인정보 처리방침에 정하여 공개하고, 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알려야 한다.----------.

V. 우리나라의 개인정보보호법제의 문제점과 전면적 개선 방안

1. 우리나라 개인정보보호법제의 문제점

가. 개인정보보호원칙이 실종되고 형해화된 규정만 남음

- 개인정보보호법이 원칙이 실종되고, 형해화되고 있음
- 개인정보보호의 원칙 : 최소수집, 목적 명확화, 익명처리 원칙 등. 선언적 규정으로 그침.

나. 개인정보처리자에게 치우친 감독기관 및 집행체계의 문제

- 방송통신위원회, 행자부, 금융위원회는 개인정보처리자에게 치우쳐 있음
  - 위법적인 가이드라인을 제정하는 등 법률을 집행할 수 없음.
  - 감독권한을 행사하지 않음
- 효과적인 감독권한 행사를 위한 체계 필요함

다. 위험 기반 접근(risk-based approach) - 비례적인 법률상 의무(scalable legal obligation), 책임성 원칙의 격상

(1) 우리나라 개인정보보호법제

– 우리 개인정보보호법은 개인정보처리자에 대하여 거의 동일한 형식적규율

• 개인정보보호법 제3장(개인정보의 처리), 제4장(개인정보의 안전한 관리), 제5장(정보주체의 권리보장)

– 안전조치 의무(제29조)도 매우 형식적임.

> 제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

– 개인정보영향평가는 공공기관 외에는 의무 없음(제33조)

– 우리 개인정보보호법의 책임성의 원칙

• “개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.”

• 형해화된 규정

(2) 유럽연합의 GDPR의 접근

– 책임성의 원칙의 재발견(책임성의 원칙(principle of accountability)에 대한 의견서(2010. 7. 13. Opinion 3/2010)

• 지속적인 의무 이행, 의무 이행을 설명할 수 있어야 함.

– 위험 기반 접근, 비례적 법률상 의무

• 개인정보 처리자의 규모나 범위에 따라서 책임의 범위도 달라져야 함.

• 제24조(정보처리자의 의무), 제32조(보안에 관한 의무), 제35조(영향평가), 제25조(프라이버시 중심 설계), 제30조(문서화 의무), 제38조, 제39조[16]

• 유럽연합 29조 작업반의 의견, 성명

▷ 책임성의 원칙(principle of accountability)에 대한 의견서(2010. 7. 13. Opinion 3/2010) : 이 의견서에서 비례성을 책임성 원칙의 중요한 내용으로 언급함.
▷ 개인정보처리자의 법률 준수는 비례적인 방법으로 이루어져야 한다(2013. 2. 27. 성명)
▷ 개인정보 보호 법률 체계에서 위험 기반 접근의 역할에 대한 성명(2014. 5. 30.)

- Directive에서도 비례성의 원칙이 있었음(“adequate", "appropriate", "reasonable" and "necessary”)
- GDPR의 비례적 법률상 의무의 적용예
  • 개인정보 영향평가
  • 프라이버시 중심 설계
  • 개인정보 침해 통지제도
  • 안전조치
  • 인증
  • 문서화 의무
- 위험의 고려
  • 위험 : 개인정보주체의 권리, 자유, 이익에 부정적 영향을 줄 수 있는 가능성과 관련된 것. 개인정보의 성질(민감정보 여부), 개인정보주체의 범주(미성년 여부), 영향 대상인 개인정보주체의 수, 처리의 목적 등의 요소를 고려. 개인정보주체의 권리와 자유에 영향을 미칠 가능성과 심각성.
  • GDPR은 ~를 고려하여(‘take into account’)라는 표현을 55회 사용함.
  • 영향을 받는 정보주체의 권리와 자유의 내용도 주된 고려 요소가 되어야 함.

16) 개인정보 보호 법률 체계에서 위험 기반 접근의 역할에 대한 성명(2014. 5. 30.)

– 특별한 위험이 확인되는 경우에는 추가적인 의무나 조치(영향 평가, 보안 조치의 강화, 개인정보 침해 통지 등)를 취해야 하고, 개인정보감독기구가 협의할 수 있는 권한이 주어짐(제34조).

제24조 정보처리자의 책임
1. 정보처리자는 처리의 성격과 범위, 상황, 목적뿐 아니라 개인의 권리와 자유의 변경 가능성과 중대성의 위험성을 참작하여, 개인정보의 처리가 본 규정을 준용하여 수행되는 것을 보장하고 이를 입증할 수 있는 적절한 기술 및 관리조치를 이행해야 한다. 이러한 조치는, 필요 시, 검토되고 업데이트 되어야 한다.
2. 처리활동과 관련하여 비례하는 경우, 제1항에 규정된 조치는 정보처리자의 적절한 개인 정보보호 정책의 이행을 포함해야 한다.
3. 제40조에 규정된 공인된 행동강령의 준수 또는 제42조에 규정된 공식 인증 메커니즘은 정보처리자의 의무의 준수를 입증하기 위한 요소로 이용될 수 있다.

제32조 처리의 보안
1. 최신 기술, 이행 비용, 처리의 성격과 범위, 상황, 목적뿐 아니라 개인의 권리 및 자유에 대해 발생할 수 있는 변경 가능성과 중대성의 위험성을 참작하여 정보처리자와 수탁처리자는 특히 아래의 조치를 비롯하여 위험에 적합한 보안 수준을 보장하는데 적절한 기술 및 관리조치를 실행해야 한다.
(a) 개인정보의 가명처리 및 암호처리
(b) 처리 시스템 및 서비스의 지속적 기밀성과 무결성, 가용성, 복원력을 보장할 수 있는 능력.;
(c) 물리적 사고나 기술적 사고가 발생하는 경우 개인정보에 대한 가용성 및 열람을 시의 적절하게 복원 할 수 있는 능력
(d) 정기적인 검사(testing), 평가 및 해당 처리의 보안을 보장하기 위한 기술 및 관리조치의 효용성에대한 평가를 위한 과정.
2. 적절한 보안 수준을 평가할 때는 처리로 인해 발생하는 위험요소, 특히 이전, 저장 또는 다른 작업으로 처리된 개인정보에 대한 사고적 또는 불법 파기, 손실, 변경, 무단 제공, 무단 열람에 대해 고려해보아야 한다.
3. 제40조에 규정된 공인된 행동강령이나 제42조에 규정된 공식 인증 메커니즘에 대한 준수는 본 조문의 제1항에 규정된 요건의 준수를 입증하는 요소로 이용될 수 있다.
4. 정보처리자와 수탁처리자는 정보처리자나 수탁처리자의 권한에 따라 개인정보를 열람하 는 모든 개인이 정보처리자의 지시에 따른 경우를 제외하고는 개인정보를 처리하지 못하도록 보장하며, 해당 개인이 유럽연합 또는 회원국 법률에 요구에 따라 처리한 경우는 예외로 한다.

제3절 개인정보보호 영향평가 및 사전 자문
제35조 개인정보보호 영향평가

1. 처리의 성격과 범위, 상황, 목적을 참작하여, 특히 신기술을 사용하는 처리 유형이 개인의 권리와 자유에 중대한 위험을 초래할 수 있는 경우, 정보처리자는 정보를 처리하기 전에 개 인정보의 보호에 대한 예상되는 처리 작업에 대한 영향평가를 수행해야 한다. 한 번의 평가 를 통해 유사한 중대한 위험을 초래하는 비슷한 일련의 처리 작업을 해결할 수 있다.
2. 정보처리자는 개인정보보호 담당관이 지정된 경우, 개인정보보호 영향평가를 수행할 때, 담 당관의 조언을 구한다.
3. 제1항에 규정된 개인정보보호 영향평가는 특히 다음 각 호의 경우 요구되어야 한다.
(a) 프로파일링 등의 자동화 처리에 근거한, 개인에 관한 개인적 측면에 대한 체계적이고 광 범위한 평가이며 해당 평가에 근거한 결정이 해당 개인에게 법적 효력을 미치거나 이와 유 사하게 개인에게 중대한 영향을 미치는 경우
(b) 제9조 (1)항에 규정된 특정범주의 개인정보에 대한 대규모 처리나 제10조에 규정된 범 죄 경력 및 범죄 행위에 관련된 개인정보에 대한 처리 또는
(c) 공개적으로 접근 가능한 지역에 대한 대규모의 체계적 모니터링.
4. 감독기관은 제1항에 따라 개인정보보호 영향평가의 요건이 적용되는 처리 작업의 종류의 목 록을 제정 및 공개한다. 감독기관은 제 68조에 규정된 유럽정보보호이사회에 해당 목록을 통보 한다.
5. 감독기관은 개인정보보호 영향평가가 요구되지 않는 처리 작업의 종류의 목록 또한 제정 및 공개할 수 있다. 감독기관은 유럽정보보호이사회에 해당 목록을 통보한다.
6. 제4항 및 제5항에 규정된 목록을 채택하기 이전에, 관련 감독기관은 해당 목록이 복수의 회 원국 내의 정보주체에게 재화와 서비스를 제공하거나 그들의 행동을 모니터링 하는 것과 관련 된 처리활동에 관계가 있는 경우, 또는 유럽연합 내 개인정보의 자유로운 이동에 중대 한 영향 을 미칠 수 있는 처리활동과 관련 있는 경우, 제 63조에 규정된 일관성 메커니즘을 적용해야 한다.
7. 평가는 최소한 다음의 각 호를 포함해야 한다.
(a) 가능한 경우, 정보처리자가 추구하는 정당한 이익을 포함한 예상되는 처리 작업과 처리 목 적에 대한 체계적인 설명
(b) 목적과 관련한 처리 작업의 필요성과 비례성에 대한 평가
(c) 제1항에 규정된 정보주체의 권리와 자유에 대한 위험의 평가
(d) 정보주체 및 기타의 관련 개인의 권리와 정당한 이익을 고려하여, 개인정보보호를 보장 하고 본 규정의 준수를 입증하기 위해, 안전조치, 보안조치 및 메커니즘 등, 위험을 해결하 기 위해 예상되는 조치.
8. 특히 개인정보보호 영향평가를 위해 관련 정보처리자나 수탁처리자가가 수행하는 처리 작업 의 영향을 평가할 때는 해당 정보처리자나 수탁처리자가 제40조에 규정된 공인된 행동 강령의 준수여부를 고려해야 한다.
9. 적절한 경우, 정보처리자는 상업적 이익이나 공익의 보호 또는 처리 작업의 보안을 침해 하 지 않고, 예정된 처리에 대한 정보주체 또는 정보처리자의 대리인의 의견을 구해야 한다.
10. 제6조 (1)항의 (c) 또는 (e)에 따른 처리가 정보처리자에 적용되는 유럽연합 또는 회원국 법률 내에 법적 근거를 두고 있는 경우, 해당 법률은 특정 처리 작업이나 일련의 해당 작업 을

규제하고 개인정보보호 영향평가는 해당 법적 근거를 채택하는 상황인 경우, 일반적인 영향평가의 일부로 이미 수행된 것이므로, 제1항에서 제7항까지 적용되지 않는다. 단, 회원 국이 처리활동 이전에 이러한 영향평가의 수행이 필요하다고 고려하는 경우는 예외로 한다.
11. 정보처리자는 처리 작업으로 초래되는 위험이 변경되는 경우, 필요한 경우, 처리가 개인정보보호 영향평가에 따라 수행되는 지 여부를 평가하기 위한 검토를 최소한 시행해야 한 다.
제36조 사전 자문
1. 제35조에 따라 수행된 개인정보보호 영향평가에서 해당 처리에 위험을 완화하고자 하는 정보처리자의 조치가 부재할 경우, 해당 처리가 중대한 위험을 초래할 수 있다고 하는 경우, 정보처리자는 처리 이전에 감독기관에 자문을 구해야 한다.
2. 감독기관이 제1항에 규정된 예정된 처리가 본 규정을 침해할 수 있다는 의견을 내놓는 경우, 특히 정보처리자가 해당 위험을 충분히 확인하지 못했거나 완화하지 못했다고 판단하 는 경우, 해당 감독기관은 자문 요청을 받은 후 최대 팔 주 이내에 정보처리자에게 서면으 로 자문을 제공해야 하며, 수탁처리자에게 적용 가능한 경우, 제58조에 규정된 일체의 권한 을 행사할 수 있다. 본 기간은 예정된 처리의 복잡성을 참작하여 6주간 추가로 연장할 수 있다. 감독기관은 정보처리자에게, 가능할 경우 수탁처리자에게, 지연된 이유와 함께 자문요 청 이후 한 달 이내에 이러한 기간연장에 대해 통지해야 한다. 해당 기간은 감독기관이 자 문 목적으로 요청한 정보를 입수할 때까지 중지될 수 있다.
3. 제1항에 따라 감독기관에 자문을 구하는 경우, 정보처리자는 다음 각 호를 감독기관에 제공해야 한다.
(a) 가능한 경우, 관련 처리에 관련된 정보처리자, 공동 정보처리자 및 수탁처리자의 개별 책임 특히 사업체집단 내의 처리에 대한 책임
(b) 예정된 처리의 목적 및 수단
(c) 본 규정에 따라 정보주체의 권리와 자유를 보호하기 위해 제공되는 조치 및 안전조치
(d) 가능한 경우, 개인정보보호 담당관의 상세 연락처
(e) 제35조에 규정된 개인정보보호 영향평가
(f) 감독기관이 요청한 기타 정보.
4. 회원국은 자국 의회가 채택하는 입법 조치에 대한 제안서 또는 이러한 입법 조치에 근거 한 처리에 관련된 규제조치를 준비하는 동안 자문기관의 자문을 구한다. 5. 제1항에도 불구하고, 회원국 법률은 사회 보호 및 공중 보건과 관련된 처리 등, 공익을 위해 정보처리자가 진행하는 업무의 수행을 위한 처리와 관련하여, 정보처리자가 감독기관 에게 자문을 구하고 사전 승인을 획득하도록 요구할 수 있다.

(3) 법률 개정의 필요성

- 우리나라의 경우도 이와 같은 규율을 도입할 필요가 있음.
- 개인정보처리자의 책임, 개인정보영향평가, 프라이버시 중심 설계, 안전조치 의무 등.

라. 전면적 법률 개정 필요 - 종합적 접근이 필요함

- 개인정보주체의 통제권 강화
- 이를 위한 투명성 강화
- 개인정보 보호 친화적인 기술 발전 , 개인정보 주체 권리구제 등을 위한 법제도의 전면적인 개편이 필요함

마. 경직된 형식적인 법률 규정의 완화

- 일부 개인정보의 처리자 입장에서 경직된 규정이 있는 것도 사실임. 예를 들어 개인정보개인정보 수집, 제3자 제공과 관련 동의가 필요 없는 경우에 대한 규정이나, 민감정보의 이용에 대한 규정 등. 공중 보건 등의 공익적 연구 목적의 개인정보 활용에 대한 예외 규정 등.
- 기타

2. 개인정보 보호원칙을 보완, 구체화하고, 실질적인 규범력을 갖도록

가. 개인정보 보호원칙은 매우 중요한 역할

- 개인정보자기결정권은 헌법으로부터 파생한 권리
- 이익형량을 해야 할 상황이 많아짐. 이런 상황에서 개인정보보호 원칙은 아주 중요한 역할

나. 개인정보 보호원칙을 구체화하고, 실질적 규범으로 개정해야 함

(1) 현재의 상태

- 현행 법률은 개인정보보호원칙을 선언적 규정으로 두고 있음.
- 제3조에서 규정하고 있는 사항을 개인정보처리자가 위반했을 경우 효과에 대해서 규정이 없음.
- 처벌 규정도 없음.
- 동의와 개인정보 보호 원칙의 관계도 규율하지 않음.

> 제3조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
> ② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
> ③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
> ④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
> ⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
> ⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
> ⑦ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.
> ⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

- '최소수집의 원칙', '목적 명확성의 원칙', '사생활 침해 최소화 처리 원칙', '익명처리의 원칙' 등이 현실에서 유명무실해 짐.
  - 감독기관에서 개인정보 보호원칙 위반을 방치하고 있는 현실이 큰 역할을 하고 있음.

(2) GDPR의 경우

- GDPR은 '적법성, 공정성, 투명성', 목적 제한, 데이터 최소화, 정확성, 보관기간 제한, 무결성과 기밀성, 책임성을 규정하고 있음[17].

(3) 최근의 대법원 판결

- 최근 대법원 판결(경품 응모권 1mm 고지 형사 사건)은 개인정보 보호 원칙을 구체적 의무로 평가하고, 해석 기준으로 제시함.
  - 이는 개인정보처리자가 정당한 목적으로 개인정보를 수집하는 경우라

---

17) GDPR 5조 개인정보처리에 관한 원칙

1. 개인정보는:

(a) 정보주체에 대해 합법적으로, 공정하게, 투명한 방식으로 처리되어야 한다('적법성, 공정성, 투명성').

(b) 명시적이고 적법한 특정목적을 위해 수집되어야 하고, 해당 목적과 양립(compatible)하 지 않는 방식으로 추가 처리 되어서는 아니된다; 공익적인 기록 보존, 과학 및 역사 연구 또는 통계 목적을 위하여 개인정보를 추가 처리한 때는 제89조 (1)항에 따라 원래의 목적과 양립된다고 본다('목적 제한').

(c) 처리되는 목적에 필요한 범위에서 적절하고 타당하게 제한되어야 한다('데이터 최소화').

(d) 정확성과, 필요한 범위에서의 최신성이 보장되어야 한다. 처리 목적에 부정확한 개인정 보는 지체 없이 삭제 또는 정정되도록 합리적인 일체의 조치가 취해져야 한다('정확성').

(e) 처리목적 달성을 위한 필요한 기간에 한해서 정보주체를 식별할 수 있는 형태로 보관되어야 한다; 정보주체의 권리와 자유를 보호하기 위하여 적절한 기술적·관리적 조치를 규정하 고 있는 제89조 (1)항에 따라, 공익적인 기록보존, 과학 및 역사연구 또는 통계목적을 위해 개인정보를 처리하는 경우, 해당 개인정보는 보유기간이 연장될 수 있다('보관기간 제한').

(f) 적절한 보안을 보장하는 방식으로 처리해야 한다. 보장하는 방식은, 적절한 기술적·관리 적 조치를 이용하여, 개인정보가 무단으로 또는 불법적으로 처리된다거나 사고로 인해 소실, 파기, 손상되었을 경우의 보호조치 등을 포함한다. ('무결성과 기밀성')

2. 정보처리자는 제1항의 사항을 준수하도록 책임을 지며, 준수한다는 사실을 입증할 수 있어야 한다('책임성')(번역 출처 : 개인정보보호위원회)

하더라도 그 목적에 필요한 최소한의 개인정보 수집에 그쳐야 하고 이에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 안 된다는 **개인정보 보호 원칙**(개인정보 보호법 제3조 제1항)과 개인정보 보호법 규정에 **위반되는 것이다**. (중략) 피고인들이 이와 같은 행위를 하면서 **개인정보 보호법상의 개인정보 보호 원칙 및 제반 의무를 위반한 점**(하략) (대법원 2017. 4. 7. 선고 2016도13263 판결).

• 대법원은 '개인정보 보호 원칙을 위반한 점'이라고 하여, 개인정보 보호 원칙 위반을 별도로 평가하였음. 이는 개인정보 보호 원칙이 단순한 선언 규정이 아니라 구체적인 의무임을 밝힌 것임.

다. 투명성의 원칙

(1) 투명성의 의미와 역할

- 정보의 불균등을 해소할 수 있는 중요한 규정
- 특히 빅데이터 활용의 환경에서 중요한 의미를 가짐.

(2) 투명성에 대한 GDPR의 규정

- GDPR의 투명성에 대한 규정
  • 제5조 : 개인정보처리에 관한 원칙
  • 제3장 제1절 투명성 및 형식
  • 제12조 : 정보주체의 권리를 행사하기 위한 투명한 정보, 통지 및 형식
  • 제13조 : 정보주체로부터 개인정보를 수집하는 경우, 제공되는 정보
  • 제14조 : 정보주체로부터 개인정보가 수집되지 않은 경우 제공되는 정보
- 투명성이 명시된 규정

- 제26조 : 공동 정보처리자
- 제40조 : 행동강령
- 제41조 : 공인된 행동강령의 모니터링
- 제42조 : 인증
- 제43조 : 인증기관
- 제53조 : 제88조 : 고용에서의 정보처리

라. 원칙의 재검토

(1) 목적 명확성의 원칙

(2) 투명성의 원칙

(3) 최소수집의 원칙

(4) 익명처리의 원칙

(5) 사생활 침해 최소화의 처리 원칙

마. 법률 개정의 방안

- 법률의 규정에 개인정보 보호원칙이 각 규정을 해석하는 기준이 된다는 점을 명시하고,
- 투명성 원칙을 명시할 필요
- 최소수집의 원칙, 목적 명확성의 원칙, 사생활 침해 최소화 처리 원칙, 익명처리의 원칙의 내용을 좀 더 구체화할 필요.
- 해당되는 관련규정에도 원칙의 내용을 포함시켜서 법률 개정을 하는 것이 바람직함.

3. 개인정보 주체의 동의와 관련하여

가. 홈플러스 경품응모권 1mm 고지 사건

- 1, 2심은 홈플러스 경품응모권 1mm 고지사건에서 동의가 적법하다고 봄
- ‘피고인 1 등과 피고인 9 회사는 개인정보 보호법상 개인정보 수집 및 그 처리에 관한 동의를 받을 때 정보주체에게 알려야 하는 사항을 응모권에 모두 기재하였다. 피고인 9 회사가 개인정보를 ‘유상으로’ 제3자에게 제공한다는 사실까지 알려야 할 의무를 부담한다고 볼 수 없고, 그와 같은 사항은 응모자들의 동의 여부 결정에 영향을 미치는 핵심적인 사항으로 보이지도 않는다. 응모권에 기재된 약 1mm 크기의 글씨는 복권, 의약품 사용설명서 등 다양한 곳에서 통용되는 것으로 경품행사 응모자들도 읽을 수 있었던 것으로 보이고, 응모함 옆에 응모권 확대 사진을 부착한 점 등에 비추어 볼 때 피고인 9 회사가 의도적으로 글씨 크기를 작게 하여 그 내용을 읽을 수 없도록 방해하였다고 보기도 어려우며, 응모자들은 자신들의 개인정보가 보험회사에 마케팅 목적으로 제공된다는 사실을 충분히 인식할 수 있는 상태에서 그에 관한 동의를 하였다고 봄이 상당하다.’고 동의가 적법하다고 보았음(서울중앙지법 2016. 8. 12. 선고 2016노223 판결).

나. 형해화된 동의의 폐해에 대한 두 가지 접근

- 규제완화론 : 규제완화론은 동의가 형식적으로 이루어지고 있기 때문에 ‘개별적 사전동의형(Opt-In) → 포괄동의(One Click Consent)+사후동의

배제(Opt-Out)로 개인정 보보호를 실질화하자'는 주장을 함. 그리고 정부가 약관심사하듯 개인정보처리방침을 심사해서 시정명령을 내리고, 법원의 사법심사를 통해 합리적인 법리를 발전시켜 나가자는 주장을 함[18].

- 동의권 보장론 : '개인정보처리자가 서면 등으로 정보주체의 동의를 받을 때 중요한 내용은 부호, 색채 및 굵고 큰 문자 등으로 명확히 표시하여 알아보기 쉽게 표시하도록 명시하도록' 하는 개인정보보호법 개정안도 제안되어 있음.

다. GDPR은 동의 요건을 강화함

(1) 동의의 정의

- GDPR은 동의를 "동의는 정보주체가 본인과 관련된 정보처리에 대하여 합의한다는 희망을 자유롭게, 구체적으로, 정보주체에게 사전에 알려진 사항에 대해 모호하지 않도록 나타낸 진술 또는 명백하고 적극적인 의사표시를 말한다."고 정의

(2) 동의의 조건

- GDPR은 동의의 조건도 명확하게 규정하고 있음

제7조 동의의 조건 1. 처리가 동의를 기반으로 이루어지는 경우, 정보처리자는 정보주체가 본인의 개인정보 처리에

18) 구태언, IoT 시대 개인정보보호를 위한 개인정보 정의, 동의제도, 시정제도 개선 제안(2015), 구태언, 빅데이터, AI 시대 개인정보의 안전한 활용을 위한 법제도 개선과제 토론문(2017. 7. 5.)

동의하였음을 입증할 수 있어야 한다.
2. 정보주체가 서면으로 동의하는 경우로 서면에 다른 사안들도 관련되어 있을 때, 동의에 대한 요청은 다른 사안들과는 명확하게 구분되는 방식으로, 이해하기 쉽고 손쉽게 접근할 수 있는 양식으로, 명확하고 평이한 문구를 사용하여 제시되어야 한다. 본 법 규정을 침해하는 어떤 선언도 구속력이 인정되지 않는다.
3. 정보주체는 언제든지 본인의 동의를 철회할 권리를 가진다. 이는 철회 이전에 동의를 기반으로 하여 이미 처리된 사항의 적법성에 대하여는 영향을 미치지 않는다(철회 전 기처리된 사항은 그대로 적법하다). 정보주체는 동의를 제공하기 전에 이 사실에 (동의를 철회할 권리 및 동의한 처리에 대한 적법성에 영향이 미치지 않음) 대하여 고지 받아야 한다. 동의의 철회는 동의의 제공만큼 용이해야 한다.
4. 정보주체의 자유로운 의사에 의하여 이루어졌는지 평가하는 경우, 특히 계약 이행에 필수적이지 않은 개인정보를 처리함에 있어 정보주체가 동의해야 한다는 조건으로 하여 서비스를 제공한다는 등 해당 계약이 이행되었는지는 않은지 면밀히 고려해야 한다[19].

라. 현재의 개인정보보호법령의 동의에 대한 규정

(1) 명확하게 인지할 수 있게 알리고 –동의의 적법 요건에 대한 규정 미흡

- 모든 동의에 적용되는 동의의 정의 규정은 없음.
- 현재의 법령은 ‘각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다.’는 규정을 두고, 개인정보 구분(정보주체와의 계약 체결 등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다.)을 규정하고,
- 선택 정보 동의 거부로 서비스 제공 거부 금지, 서면, 우편, 팩스, 전화, 인터넷 홈페이지 표시하도록 하는 등 주로 표시의 방법에 국한하고 있음,

19) 번역 출처 : 개인정보보호위원회

- 홍보 및 판매권유 목적 개인정보 처리 동의 - 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.

(2) 동의의 조건 - 투명성과 자발성에 대한 규정 추가할 필요

- 적법한 동의가 되기 위한 요건을 좀 더 명확하게 규정할 필요가 있음. 특히 투명성에 관한 규정을 둘 필요가 있음.
- 동의의 자발성과 자유에 대한 규율을 둘 필요가 있음.

(3) 개인정보보호의 다른 원칙을 위반하는 것이면 동의가 있어도 적법한 개인정보 처리의 근거가 될 수 없다는 점을 분명하게 할 필요

- 현행 법률 규정은 동의에도 불구하고 최소수집의 원칙은 준수되어야 한다고 해석할 소지는 있음.
  - 개인정보보호법 제16조의 각 규정들은 동의와 최소수집의 원칙, 부가정보의 수집 가능성 등에 대해서 매우 혼란스런 규정임.
  - 최소 수집의 범위, 부가 정보는 수집할 수 있는 것인지 등[20]

---

20) 제16조(개인정보의 수집 제한) ① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.

② 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다. <신설 2013.8.6>

③ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다. <개정 20

- 그러나 개인정보보호의 원칙과 동의의 관계를 명확하게 밝히고 있지 않음.
- 개인정보보호 원칙에 위반되는 개인정보 처리는 동의가 있어도 위법하다고 보아야 함. 이를 명확하게 밝힐 필요

4. 프로파일링과 자동화된 결정에 대한 규정[21)]

가. 유럽연합 GDPR의 규정

(1) 프로파일링의 정의

- “프로파일링”이란 개인을 평가하거나, 개인의 업무실적, 경제상태, 위치, 건강, 선호, 신뢰성이나 행동 등을 분석 또는 예측하기 위해 이루어지는 개인정보의 자동화된 처리를 말한다.

(2) 개인정보주체에게 고지할 사항

- 개인정보 수집시 프로파일링, 자동의사결정의 유무 등에 관한 정보를 고지해야 함.
  - 프로파일링 등 자동 의사결정의 유무, 관련 논리(logic)에 관한 유의미한 정보, 프로파일링에 따라 이루어지는 조치, 프로파일링에 의해 해당 정보주체에게 예상되는 효과

13.8.6>

21) GDPR 22조 등(번역 출처 : 개인정보보호위원회)

• 개인정보를 자동화하여 처리하는 경우 처리 기준에 대한 정보

(3) 프로파일링 등 자동화된 결정에 대한 거부권

- 정보주체는 본인에 관한 법적 효력을 초래하거나 이와 유사하게 본인에게 중대한 영향을 미치는 자동 처리에만 의존하는 프로파일링 등의 결정의 적용을 받지 않을 권리를 갖는다. 단, 아래 세 가지의 경우는 제외.
  • 정보주체와 정보처리자 간에 계약을 체결 또는 이행하는데 필요한 경우 (이 경우 정보처리자가 정보주체의 권리 및 자유와 정당한 이익, 최소한 정보처리자의 인적 개입을 확보하고 본인의 관점을 피력하며 결정에 대해 이의를 제기할 수 있는 권리를 보호하는데 적합한 조치를 시행해야 함)
  • 정보처리자에 적용되며, 정보주체의 권리와 자유, 정당한 이익을 보호하기 위한 적절한 조치에 대해 규정하는 유럽연합 또는 회원국 법률이 허용하는 경우
  • 정보주체의 명백한 동의에 기반하는 경우(이 경우도 정보처리자가 정보주체의 권리 및 자유와 정당한 이익, 최소한 정보처리자의 인적 개입을 확보하고 본인의 관점을 피력하며 결정에 대해 이의를 제기할 수 있는 권리를 보호하는데 적합한 조치를 시행해야 함).
- 민감정보에 기반한 결정은 당사자의 명시적 동의가 있거나, 법률에 규정된 중대한 공익을 위해 필요한 경우이고, 정보주체의 권리와 자유, 정당한 이익을 보호하는 적절한 조치가 시행되는 경우 외에는 허용되지 않는다.

나. 프로파일링, 자동화된 결정에 대한 규정의 필요성과 도입 방안

- 프로파일링과 자동화된 결정과 관련된 규정은 빅데이터 정보처리의 시대에 개인정보주체의 권리를 보장하기 위한 가장 중요한 규정임.
- 이에 대한 규율을 개인정보보호법제에 도입해야 함.

5. 개인정보 이전권

가. GDPR의 규정

본인의 개인정보 이전권[22)]
1. 정보주체는 정보처리자에게 제공한 본인에 관련된 개인정보를 체계적으로 작성되고 일반 적으로 사용되며 기계 판독이 가능한 형식으로 수령 받을 권리가 있으며, 개인정보를 제공 받은 정보처리자를 방해하지 않고 다른 정보처리자에게 해당 개인정보를 이전할 권리를 갖는다.
(a) 제6조 (1)항의 (a)나 제9조 (2)항의 (a)에 따른 동의나 제6조 (1)항의 (b)에 따른 계약을 기반으로 하는 처리의 경우
(b) 자동 수단을 통해 처리가 수행되는 경우.
2. 제1항에 따른 본인의 개인정보 이전권을 행사하는 데 있어, 기술적으로 가능한 경우, 정 보주체는 해당 개인정보를 한 정보처리자에서 다른 정보처리자로 직접 이전하게 할 권리를 갖는다.
3. 본 조문의 제1항에 규정된 권리의 행사는 제17조를 침해해서는 아니된다. 해당 권리는 공익상의 업무를 수행하기 위해 또는 정보처리자에게 부여된 공식 권한의 행사를 위해 필 요한 처리에는 적용되지 않는다.
4. 제1항에 규정된 권리는 다른 개인의 권리와 자유를 침해하지 않아야 한다.

22) GDPR 제20조(번역 출처 : 개인정보보호위원회)

나. 의미[23]

- 정보주체가 정보저리자에게 제공한 개인정보를 체계적이고 통용되며 기계 판독이 가능한 형태로 제공받고 다른 정보처리자에게 방해없이 해당정보를 이전하는 것을 가능하게 해 주는 권리
- 이 새로운 권리는 정보주체에게 본인의 정보와 관련된 권한을 부여하여 한 IT 환경에서 다른 IT 환경으로 본인의 정보를 쉽게 이동시키거나 복사, 이전 시킬 수 있도록 함. 개인 소유의 장비 또는 클라우드에 저장할 수 있음.
- 정보이전권은 정보주체와 정보처리자 간의 관계가 재균형(re-balance)을 이루도록 기회를 제공함.
- 열람권을 보완하는 기능.
- 개인의 정보이전권 행사시 개인은 기타 권리를 침해하지 않아야 함. 정보주체는 정보처리자의 서비스를 계속해서 사용하고 혜택을 받을 수 있으며 이는 정보이전이 이루어진 후에도 마찬가지. 정보주체는 정보처리자가 정보를 처리하는 한 본인의 권리를 행사할 수 있음.

다. 필요성

- 우리 환경에서 매우 중요한 권리임.
- 개인정보주체의 통제권을 실질적으로 보장하는 역할을 할 것임.

---

23) 유럽연합 WP 29의 정보이전권(Right to Data portability)에 관한 가이드라인(번역 출처 : 개인정보보호위원회)

6. 프라이버시 중심 설계

가. GDPR의 규정

제25조 개인정보보호 중심 디자인 및 설정 1. 최신 기술과 실행 비용, 처리의 성격과 범위, 상황, 목적뿐 아니라 처리로 인해 개인의 권리와 자유에 대해 발생할 수 있는 변경 가능성과 중대성의 위험성을 참작하여, 정보처리자 는 처리 수단을 결정한 시점과 처리 당시 시점에서, 데이터 최소화 등 개인정보보호의 원칙을 이행하고 본 규정의 요건을 충족하고 정보주체의 권리를 보호하기 위해, 처리에 필요한 안전조치를 포함하기 위해 고안된 가명처리 등, 적절한 기술 및 관리조치를 이행해야 한다. 2. 정보처리자는 기본설정을 통해, 처리의 개별 특정목적에 필요한 정도에 한하여 개인정보 가 처리될 수 있도록 보장하기 위한 적절한 기술 및 관리조치를 이행해야 한다. 이러한 의 무는 수집되는 개인정보의 양, 해당 처리의 범위, 개인정보의 보관기간 및 접근용이성에 적 용된다. 특히, 이러한 조치는 개인정보가 관련 개인의 개입 없이 불특정 다수에게 열람되지 않도록 기본설정을 통해 보장한다. 3. 제42조에 근거한 공식 인증 메커니즘은 본 조항의 제1항 및 제2항에 규정된 요건의 준수를 입증하는 요소로 이용될 수 있다.

나. 의미[24)]

- 개인정보보호 중심 디자인 및 설정은 개인정보처리자가 준수해야 할 기술적, 관리적 조치의 하나임.

• 정보처리자는 개인정보보호 중심 디자인 및 설정의 원칙을 충족하는 내부 정책과 조치를 채택하고 시행해야 함.

• 이 조치는 개인정보처리의 최소화, 가능한 빠른 시일 내의 개인정보의 가명처리, 개인정보의 기능 및 처리의 투명성 제고, 정보주체의 개인정보처리에 대한 감시와 정보처리자의 보안 대책의 수립 및 개선으로 구성될 수

24) GDPR Recital 78(번역 출처 : 개인정보보호위원회)

있음.

- 제품, 서비스, 어플리케이션 개발자의 권장 의무

• 개인정보처리에 근거하거나 관련 업무를 위해 개인정보를 처리하는 어플리케이션, 서비스 및 제품을 개발, 디자인, 선택 및 이용할 때, 해당 제품, 서비스 및 어플리케이션의 제작자는 관련 제품, 서비스 및 어플리케이션을 개발하고 디자인할 때 개인정보보호권을 고려하고 정보처리자와 수탁처리자가 개인정보보호 의무를 준수할 수 있도록 보장하도록 권장된다.

- 개인정보보호 중심 디자인 및 설정의 원칙은 공개입찰 상황에서도 고려되어야 한다.

다. 필요성

- 우리나라 개인정보 보호법제에서도 필요한 규정임.

7. 그 외

- 그 외에도 개인정보주체에 대한 동의시 고지, 통지, 수집 후 고지 사항 등의 보완.
- 개인정보 영향평가와 감독기구의 관여
- 개인정보 감독기구의 권한 강화
- 개인정보 주체에 대한 구제수단 등이 보완되어야 함.

메모

메모

메모

메모