경북대학교 법학연구원『법학논고』
제61집 (2018.04) 81~115면.
Kyungpook Natl. Univ. Law Journal
Vol.61 (Apr 2018) pp.81~115.

유럽연합과 독일의 개인정보보호법의 비판적 수용을 통한 우리나라의 개인정보보호법의 입법개선을 위한 소고*

임 규 철**

〈국문초록〉

유럽연합의 개인정보보호법(이하 GDPR)은 EU 거주 정보주체에게 재화 또는 서비스를 제공하거나 그 정보주체의 행동을 모니터링하는 우리나라의 개인정보처리자에게도 적용이 된다. 독일의 개인정보보호법도 동일하다. 그 개인정보처리자는 GDPR 제45조의 '적절한 보호수준', 제46조와 제49조에 따른 '적절한 안전조치' 및 '특례'의 인증을 통해 유럽인의 개인정보를 국외에서도 처리를 할 수가 있다. 감독기관의 독립성 미비로 적절성 인증을 받지 못했고 현재 정보통신망법 중심의 부분 적절성 인증을 받으려고 시도 중이다. GDPR의 개인정보 보호수준이 적절하고 유럽과 경제교류가 확대되는 상황에서 국내 사업자 부담의 경감을 위해 인증은 필요하다.

개인정보법제에서의 개인정보처리자에 대한 개념에 있어 우리의 '업무성 및 개인정보 파일' 혹은 GDPR의 '개인정보 처리의 목적 및 수단'은 삭제가 바람직하다. 복잡한 개념설정은 입법의 신뢰도에 도움을 주지를 않는다. 가족 혹은 사적인 처리 혹은 통계 등 적용배제는 별도의 규정을 통해 정립하는 것이 입법의 효율성을 위해 좋다. 개인정보 개념에 있어 GDPR 제4조 제1항의 "식별가능한 정보주체는 직접 혹은 간접적으로 특히 이름, 식별번호, 위치정보, 온라인 식별자로 알아볼 수 있거나 하나 또는 그 이상의 구체적인 요소를 통하여 정보주체의 신체적, 생리적, 경제적, 문화적, 사회적 정체성이 식별될 수 있는 자'의 입법형식을 적극적으로 수용할 필요가 있다. 이를 통해 주민등록번호 외에도 mac이나 IP주소, cookie 및 즐겨찾기 등에 대한 개인정보성 유무와 관련해서 더 이상 논란이 없이 정보주체의 보호범위를 넓힐 수가 있기 때문이다. 빅 데이터 시대에 있어 법적 안정성 유지를 위해 기준의 유동성이 심한 비식별화조치보다는 법률로 익명 및 가명정보의 법제화가 필요하다. 익명정보의 개인정보성을 부인하지만 재식별화에 대한 개인정보처리자의 위험책임을 명기할 필요가 있다. 기술의 발달로 재식별은 시간의 문제이기 때문이다. 정부주도로 일본의 '익명가공정보'의 개념을 차용해와 '비식별화조치 가이드라인'을 통해 개인정보성을 부인하고 재식별 시 즉각적인 폐기 및 유출차단 등의 조치가 있으면 면제한다고 규정을 하면서 공공기관의 개인정보 유무상의 제공이 이뤄지고 있는 것은 위임의 한계를 일탈한 것으로 위법성이 짙다.

동의는 GDPR에 따르면 정보주체가 진술(구두, 문서) 혹은 명백히 긍정적인 행

* 이 논문은 동국대학교-서울 논문 게재장려금으로 이뤄졌음.
** 동국대학교 법과대학 법학과 교수

위를 통한 본인과 관련된 개인정보 처리의 승낙을 말한다. 동의의사는 명백하게 표시되어야 한다. 침묵이나 부작위 혹은 사전에 자동적으로 존재하는 처리동의는 동의로 볼 필요가 없다. 홍보 및 상업적 판매목적인 경우에는 GDPR 및 우리 개인정보보호법의 '명백한 기회제공'과 달리 '별도의 명백한 동의'의 입법이 바람직하다. 서면동의 시 명백하고 쉬운 언어이면서 접근의 수월성과 함께 동의거절 및 철회권이 적극적으로 보장되어야 한다. 우리의 개인정보보호법은 사전동의를 지향하면서 개인정보처리자에게 필수동의 및 임의정보의 구분과 법정 동의내용 고지의무를 부과하고, 개인정보의 유상판매 시 시행규칙을 통해 글자크기 및 색깔 혹은 밑줄 등의 표시를 강제화하고 있다. GDPR 전문 43번의 '정보주체와 개인정보처리자 간에 정보처리에 있어 명백한 불균형이 존재하는 경우 동의를 처리의 합법적인 근거로 제시해서는 안 된다. 특히 개인정보처리자가 공공기관이기 때문에 동의가 자유롭게 제공될 것 같지 않은 경우이다. 별개의 개인정보 처리행위에 대해 별도의 동의를 받지 않는 경우이거나 혹은 서비스 제공 등의 계약이행이 동의가 없이 이루어질 수 있음에도 불구하고 동의에 근거하여 진행되는 경우에는 해당 동의는 자유롭게 제공된 것이라고 볼 수 없다.'는 규정은 관련 규정의 해석 시 적극적으로 참조할 필요가 있다. 위원회에 계류 중인 정보통신망법 개정안은 상업적 판매의 명시를 고지의무로 규정하고 있다.

주제어 : 정보주체, 동의, 서면동의, 익명 및 가명정보, 한국 개인정보보호법, 유럽연합의 개인정보보호법

• 투고일 : 2018.03.12. / 심사일 : 2018.04.18. / 게재확정일 : 2018.04.26.

I. 들어가면서

2011년 9월부터 개인정보보호법이 시행되고 있다. 우리의 개인정보의 보호수준이 상당한 수준에 올랐지만 그럼에도 불구하고 정보시장에서의 개인정보의 유출 및 오남용의 여전하다. 그 때문에 동 법률에 대한 평가에 있어 동의제도의 형식화 방지 및 위반 시 처벌의 강도의 미약 혹은 다수의 특별법으로 인해 일반법인 개인정보보호법으로서의 기능의 제한은 문제라는 주장과 빅 데이터 및 클라우딩 시대에 맞는 개인정보의 활용보장을 못한다는 주장이 혼재되어 있다. 서로 바라보는 방향은 틀릴지언정 개정의 필요성은 공통적이다. 빅데이터 및 클라우딩 시대라는 정보환경의 급격한 변화에 따른 관련 법제의 정비는 필수적이겠지만 '산업혁명은 뒤졌지만 정보혁명은 뒤지면 안 된다.'는 경제우선주의 입장을 개인정보법제에 그대로 도입하는 것은 문제가 된다. 개인정

보 그 자체가 인격적, 재산적, 의사소통 가치라는 종합적인 가치를 가지고 있기에 일방향적인 규정은 문제해결을 어렵게 하기 때문이다.

이 와중에 '유럽연합 개인정보보호법'(General Data Protection Regulation; Datenschutz-Grundverordnung/DSGVO, 이하 'GDPR')[1]이 2018년 5월 25일부터 시행된다. GDPR은 기존의 95/46/EU을 대체하는 규범이다. 그러나 GDPR 제94조는 '폐기된 95/46/EU에 대한 해석은 해당 GDPR적용 시 고려되어야 한다. 특히 95/46/EU의 제29조가 정한 개인정보 처리와 관련된 '작업반'(Working Party, Gruppe-29, 이하 WP-29)의 해석은 GDPR의 유럽정보보호위원회(European Data Protection Board/EDPB; Europäischen Datenschutzausschuss)에도 유효하다.'고 규정하고 있어 두 규범은 지속적으로 연결되어 있다는 것을 알 수가 있다.[2]

유럽연합 28개국 중 독일이 제일 먼저 2017년 6월 기존의 '개인정보보호법'(Bundesdatenschutzgesetz/BDSG, 이하 '현행 BDSG')을 완전 대체하는 '개인정보보호법'(Bundesdatenschutzgesetz/BDSG. 이하 '2018 BDSG')이 2018년 5월 25일부터 시행예정이다. GDPR '전문'(recital/Erwägungsgrund, 유권해석의 기준) 제41번에서는 '이 법에서 법적 근거나 법적 조치를 규정하고 있는 경우 이 규정들이 회원국의 입법과정을 거쳐 채택될 필요는 없으며, 회원국의 헌법적 질서에 따른 필수사항들을 방해하지 않는다(회원국의 입법과정을 거치지 않아도 되고 회원국 헌법질서와 병립도 가능).'라고 규정하고 있다. 2018 BDSG는 다른 27개 회원국의 개인정보보호법 개정에 상당한 파급력이 미칠 것이다. 동 법은 유럽연합의 해당 GDPR에서 각각의 회원국에게 21개 조항에서 입법형성 재량을 부여한 영역에서 자국법으로의 최초로 구체화된 법률로 충분히 다른 회원국들이 참조가 가능한 규범이고, 기존에도 유럽연합의 개인정보보호법제의 영역에서 현행 BDSG의 '자동화된 의사결정' 조항도 GDPR에 적극적으로 반영이 된 것 사례가 있었기 때문이다.[3]

---

1) Regulation(EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC(General Data Protection Regulation); Verordnung(EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG(Datenschutz-Grundverordnung).

2) 그 전반적인 흐름에 대해서는 한은영, "유럽연합(EU), 개인정보보호(Data Protection)강화 추진", 정보통신정책연구원, 동향 제26권 제7호, 2014, 32-41쪽 참조.

우리의 개인정보보호법의 개정논의에 있어 두 규범의 비판적 수용을 통한 적극적인 입법적 고려가 필요한 시기다. 우리의 민간 개인정보처리자 혹은 공공기관을 중심으로 유럽과 경제교류 확대가 되는 상황에 있어 개인정보보호가 걸림돌이 되게 할 필요는 없고, 빅 데이터 및 클라우딩 시대에 있어 두 규범의 개인정보의 보호 및 활용의 새로운 균형점은 일정 영역에 있어 우리가 수용을 할 정도의 합리성을 가지고 있다고 보기 때문이다. 특히 개인정보법제의 통합화는 법적 안정성을 통한 정보주체의 실질적인 보호를 위해 시급히 필요한 입법정책이라고 본다.[4] 그러나 비교검토를 함에 있어 GDPR이나 2018 BDSG가 이러한 방향으로 개편되었으니 우리 국내법도 자동적으로 이에 따라야 된다는 것은 결코 아니다.

이하의 내용에서는 유럽연합의 GDPR과 독일의 2018 BDSG의 내용 중 논란이 되는 적용영역, 개인정보 및 개인정보처리자, 익명 및 가명정보, 동의제도를 비판적으로 알아보면서 우리의 개인정보보호법의 입법개선 방향을 알아보고자 한다.[5] 그 외의 일반 및 민감정보의 처리, 감독기관, 배제영역 등은 다음의 연구에서 알아보기로 한다.

II. 적용대상

1. 규정

유럽연합은 개인정보 보호규정이 회원국 내에서 무역의 장벽으로 등장하는

3) 동일한 의견으로는 박노형, 「4차산업혁명 · EU GDPR 대응 개인정보보호 세미나 개최결과 종합자료집」, 개인정보보호위원회, 2017.11., 11쪽.

4) 대법원은 '법률이 상호모순 혹은 저촉되는지는 법률의 입법목적, 규정사항, 적용범위 등을 종합적으로 검토하여 판단하여야 한다.'고 보면서 그 전제조건으로 '입법목적을 달리하는 법률들이 일정한 행위에 관한 요건을 각각 규정하고 있는 경우에는 어느 법률이 다른 법률에 우선하여 배타적으로 적용된다고 해석되지 않는 이상 그 행위에 관하여 각 법률의 규정에 따른 요건을 갖추어야 한다.'고 요구하고 있지만 개인정보법제에서의 다수 특별법의 세밀한 내용은 일반법인 개인정보보호법의 적용제한 및 적용규정의 혼란을 가져오고 있다(대법원 1995.1.12. 선고 94누3216 판결; 2016.11.25. 선고 2014도14166 판결); 임규철, "정합성의 입장에서 본 개인정보보호법 제6조와 정보통신망법 제5조의 '다른 법률에(서) 특별한 규정'에 대한 소고", 서울법학 제25권 제4호, 서울시립대 법학연구소, 2018.2., 500-518쪽.

5) 유럽연합의 GDPR과 독일의 2018 BDSG의 내용은 우리의 개인정보보호위원회가 번역한 내용을 참고로 하여 기술하였다.

것을 바라지는 않는다. 그러나 현실적으로 경제적 혹은 문화적 차이가 있어 그 보호수준이 상이하기에 회원국간의 동일한 보호수준으로의 통일화라는 방법을 채택하였다. 여기에는 전문 제1번에서 언급하고 있는 것처럼 개인정보의 보호는 기본적 권리이며 이는 국적 혹은 거주지에 상관이 없이 존중되어야 한다는 생각이 전제되어 있기도 하다. 또한 정보처리 기술의 등장에 대해 긍정적으로 바라보면서 제3국 및 국제기구로의 개인정보 이전의 용이함을 담보하기 위해 공통적으로 높은 보호수준을 가져야 한다는 의식도 적용대상의 확대로 이어졌다고 판단할 수가 있다(전문 제6번)

GDPR 제3조는 '유럽연합의 비회원국에서 회원국 정보주체에 대한 정보처리 시 및 재화나 서비스 제공 시와 모니터링 시' GDPR의 적용을 명문화하고 있다. 2018 BDSG도 제1조 제4항 제3호의 '개인정보처리자 또는 수탁처리자가 유럽연합 회원국 또는 유럽경제협약국 내에서 거주하지 않는 경우에도 GDPR은 적용이 된다. GDPR의 적용이 없는 경우라도 개인정보처리자 또는 수탁처리자는 이 법률의 제8조부터 제21조, 제39조부터 제44조까지는 적용이 된다.'의 규정을 통해 자국민의 정보처리 시 제3국의 공공 및 민간부문의 개인정보처리자 또는 수탁처리자(이하 '개인정보처리자')에게도 적용이 된다. 따라서 제3국의 개인정보처리자는 각 회원국들이 유럽연합 GDPR 및 2018 BDSG의 보호수준에 맞는 개인정보보호법 및 정책을 가지고 있어야 한다. 이에 위반 시 GDPR 제83조에 따라 전체 연 매출액 2-4% 혹은 1,000-2,000만 Euro 중 무거운 액수의 과징금 부과대상이 된다.

우리의 개인정보보호법은 제5조 제1항에서 '국가와 지방자치단체는 개인정보의 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등에 따른 폐해를 방지하여 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구하여야 한다.' 및 제14조 제2항에서 '정부는 개인정보 국외이전으로 인하여 정보주체의 권리가 침해되지 아니하도록 관련 시책을 마련하여야 한다.'고 규정하고 있다. 이러한 규정이 단순한 선언규정이라고 보기는 힘들고, 대법원도 개인정보보호법 제3조 제6항의 개인정보보호원칙 중 '최소수집'에 대해 강제력이 있는 규범이라고 판단하고 있다.[6] GDPR 제5조의 처리원칙도 전문 제26번에서 명문으로 규범력을 인정하고 있기도 하다. 국외 이전되는 개인정보에 대해 좀 더 구체적

6) 대법원 2017.4.7. 선고 2016도13263 판결.

으로 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법')에 제63조에 정보통신망법에 위반되는 국제계약을 체결해서는 안 되고, 법정고지사항에 따른 고지의무 및 시행령에 보호조치를 요구하고 있다. 그러나 계약이행과 이용자 편의증진을 위해 필요한 경우로 개인정보처리방침에 공개한 경우에는 동의가 불필요함을 규정하고 있다. 재판준거권과 손해배상 혹은 감독기관의 적극적인 관여 규정이 없는 이러한 규정은 GDPR 및 2018 BDSG의 자국민의 개인정보의 국외 이전 시의 보호수준과는 차이가 크다. 즉, 국외 이전에 대한 법 및 정책의 보호수준이 우리의 수준과 맞대응 할 정도로 유효해야 한다는 규정이 없다. 보호수준이 높은 국가로의 이전은 문제가 없지만 낮은 국가로의 개인정보 이전은 문제가 된다.

2. 개선방향

유럽연합의 GDPR은 법규위반 시 국내외 구분이 없이 적용의 강제화를 위한 명문의 규정이 세세하게 있으나 우리의 관련 법제는 사실상 국내용으로 한정되어 있어 자국민의 개인정보가 국외로 이전 시 보호대책이 미비하다고 볼 수가 있어 이에 대한 적극적인 대책이 필요한 시기다.

2014년에 방송통신위원회는 '구글 street view 사건'에서도 국내법을 적용하여 과징금 부과한 사례가 있다. 2016년 서울고법도 '구글의 개인정보 제3자(NSA) 제공내역 공개 사건'에서 구글에 대한 국내법 적용을 제한적으로나마 판시하고 있다.[7] 자국민 개인정보의 국외 이전 시 보호수준을 높이기 위해 이러한 개별적인 조치보다는 일반적인 조치가 필요하다고 볼 수가 있다. 즉, 자국법의 내용을 제3국에 적용시키는 역외규정인 95/46/EU 제4조 제1항 (c)[8] 및 GDPR 제3조 및 2018 BDSG 제1조 제4항 제3호 그리고 비록 제한적이지만 일본의 제75조 및 제86조[9]의 자국민 개인정보보호라는 취지를 국내 법제도 적극

7) 서울고법 2016.12.22. 선고 2015나2065729 판결: 서울중앙지법 2015.10.16. 선고 2014가합38116 판결.

8) 95/46/EU 제4조 제1항 (c): 개인정보처리자가 공동체의 영토에서 설립되지 않으면서 개인정보 생산을 목적으로 당해 회원국에 위치한 자동화된 또는 비자동화된 장비를 이용을 하지만 당해 장비가 공동체의 영토를 통과할 목적에 한하여 사용되는 것이 아닌 경우.

9) 일본 제75조: 제15조, 제16조, 제18조(제2항을 제외한다), 제19조에서부터 제25조까지, 제27조에서부터 제36조까지, 제41조, 제42조 제1항, 제43조 및 다음 조의 규정은 국내에 있는 자에 대한 물품 또는 서비스의 제공과 관련하여 그 자를 본인으로 하는 개인정보를 취급한 개인정보취급사업자가 외국에서 당해 개인정보 또는 당해 개인정보를 이용하여 작성한

적으로 고려할 필요가 있다. 한국인의 개인정보가 국내보다 보호수준이 떨어진 국가로의 이전은 적절하게 관리를 할 필요가 있기 때문이다. 현실적으로 주요 실행기관인 행정안전부나 방송통신위원회는 유럽연합 및 독일과 일본처럼 강하게 내국인의 개인정보보호정책을 추진하고 있다고 보기는 힘들다. 한국 외에서 발생하는 한국인의 개인정보 침해구제 수단으로서 역외규정의 신설을 통해 자국민의 정보에 대해 적극적으로 보호할 필요가 있다. 행정안전부는 ISMS 및 PIMS 인증을 통한 적절성 확보 및 상호주의 입법을 검토하고 있고,[10] 방송통신위원회도 2018년 1월 전기통신사업법과 정보통신망법에 역외규정의 신설을 통해 '일정 규모 이상의 외국계 인터넷기업이 의무적으로 국내 대리인을 두도록 하고 심각한 문제를 일으키면 경우에 따라 서비스 차단이나 앱 등록 거부조치를 취할 수 있도록 하겠다.'는 입장을 보이고 있다.[11] 일반법으로의 통합법 방향이 옳다면 개인정보보호법에 관련된 규정을 신설하는 것이 옳다.

GDPR 제3조와 2018 BDSG에 따른 우선적인 주요 적용대상은 apple, google, facebook 및 twitter가 될 것이라는 예상을 하지만, 유럽연합과 경제적 교류가 확대되고 있는 국내 개인정보처리자에게도 큰 영향을 미칠 것이라고 보는 것이 합리적인 예상일 것이다. GDPR과 2018 BDSG는 제3국의 개안정보법과 정책을 통한 보호수준이 자기들과 비교해서 적절하거나 충분한 보장이 된다는 판단이 들면 자국민의 개인정보 이전 등의 처리를 허용하고 있다. 부당한 대우를 막기 위해서는 95/46/EU의 제25조 및 제26조에서 규정하고 있는 '적절한 보장'과 '충분한 보장' 규정[12]이 전환이 된 WP-29의 가이드라인을 그대로 입법화한 GDPR 제45조 및 제46조에 따른 인증을 받을 필요가 있다. 핵심은 감독기관의 독립성 확보 유무, 법률의 존재 및 실효성 유무와 규제적 자율규제(BCRs)의 존재 및 실효성 유무다.[13] 그 요구된 보장수준을 보면 형식적

익명가공정보를 취급하는 경우에 대해서도 적용한다. 제86조: 제82조 및 제83조의 규정은 일본국 외에서 이들 조의 죄를 범한 자에게도 적용한다.

10) 최경진, 「4차산업혁명ㆍEU GDPR 대응 개인정보보호 세미나 개최결과 종합자료집; EU GDPR 영향과 대응방안」, 개인정보보호위원회, 2017.11., 28쪽.

11) GDPR에 대한 국내 개인정보처리자의 대응 및 주의사항에 대해서는 KISA, 「우리 기업을 위한 GDPR 안내사항」, 2016; http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&oid=001&aid=0009812078&sid1=001(검색일: 2018.3.2.; 검색어: 역외규정)

12) 판단을 위한 실체적 및 절차적 판단기준에 대해서는 임규철, 「21세기 개인정보 정책과 법」, 북포유, 2015, 139-140쪽; Mitteilung zur 'Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU' am 24. 7.1998(http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_de.pdf) 참조.

13) 이인호, "지능정보화 사회 대응 개인정보보호 세미나 - 개인정보보호 수행체계 효율화 방

으로는 감독기관의 독립성 부족과 실질적으로는 규제적 자율규제의 약간의 실효성 부족 외에는 국내 개인정보법제가 전체적으로는 열위라고는 볼 수가 없다. 유럽연합에서 제3국으로의 개인정보 이전 시 '적절성 평가'를 신청했지만 2016년 10월 일본은 인증을 받았고 우리는 받지를 못했다.[14] 유럽연합의 '우리의 개인정보 감독기관인 개인정보보호위원회의 독립성을 약하게 보면서[15] 실질적으로는 행정안전부에서 집행감독을 하고 있다는 판단'이 주요 이유로 알려지고 있다.[16] 이후 과학기술정보통신부에서는 방송통신위원회의 독립성을 근거로 '부분 적절성' 평가를 신청 중이다. 이에 대해 개인정보보호위원회는 해당 효과의 제한성 및 개인정보보호법의 적용혼란 등을 이유로 해당 신청의 부적절성을 권고하고 있다.[17] 여기에 있어 2017년 5월 시행 중인 일본의 개정된 개인정보의 보호에 관한 법률 제59조부터 제74조에 새롭게 규정된 개인정보보호위원회에 대해 유럽연합이 판단한 '독립성의 충분한 인정 결정'이 정치적이고 경제적인 결정과 무관하다고 보기는 힘들다는 정황을 적극적으로 고려할 필요가 있다.[18] 일본의 해당 위원회는 국내 개인정보보호위원회보다는 조직적으로 내무성의 통제를 벗어났기에 독립성이 형식적으로는 낫지만 이제 시작단계이기에 실질적인 검증이 되지 않은 상태이고, 그 외에서는 한국의 개인정보보호법상 인증제도 및 개인정보영향평가, 심의평가제도, 징벌적 과징금 및 법정손해배상 제도 등에서 일본보다 전반적으로 우수하기 때문이다. 2001년 'Safe Harbor'처럼 정치 및 경제적인 고려가 우선적으로 참작된 결정일 수가

안 -", 개인정보보호위원회, 2017.12., 200-210쪽.

14) 2017년까지 '이스라엘, 캐나다, 헝가리, 스위스, 호주, 뉴질랜드, 페루' 등이 적절성 평가 인증을 받았다.

15) 감독기관의 독립성에 대한 유럽사법재판소의 판례에 대해서는 Kommission/Österreich, C 614/10, EU:C:2012:631, Rn. 36; Kommission/Ungarn, C 288/12, EU:C:2014:237; 이에 대한 요약설명 글로는 이인호, 앞의 글, 204-206쪽.

16) 개인정보보호위원회 결정 제2016-23-83호; 오병일, "지능정보화 사회 대응 개인정보보호 세미나 - 개인정보보호 법령간 정합성 강화 방안 -; 개인정보보호위원회의 독립성과 권한강화 필요성", 개인정보보호위원회, 2017.12., 240쪽.

17) 개인정보보호위원회 결정 제2017-25-198호.

18) '적절성'의 개념은 법학적 견지에서는 해석상의 문제점을 가지고 있다. 이는 각 회원국의 정치적이고 경제적인 이해타산을 고려한 합의를 이끌어 내기 위한 정치적 표현일 수가 있기 때문이다. 이에 대해서는 Ellger, Datenexpert-Rechtslage nach dem geänderten Entwurf der EG-Datenschutzrichtlinie zum Datenschutz, CR 1993, 8 f.: http://europa.eu.int/comm/internal_market/en/media/dataprot/news/harbor3.pdf; http://www.privacyinternational.org/issues/compliance/ep-safeharbor-700.html; http://europa.eu.net/comm/internal_market/de/media/dataprot/wpdocs/index.htm; Kneifel, Freedom of Information in den USA, CR 1990, 134(138).

있다. 'EU-US Safe Harbor'는 미국에서의 실질적인 개인정보의 보호가 유럽연합보다는 미약하지만 경제교류의 걸림돌 완화라는 정치적인 이유로 체결이 됐고,[19] 이에 따라 2015년 유럽사법재판소는 자국민의 정보처리에 대한 미 정보수사기관의 근거가 미약하면서도 과다한 수월성 보장 및 미 회원사의 개인정보보호의 실효성 미비와 회원국 개인정보감독기관의 재통제 불인정 이유로 'Safe Harbor'에 대해 무효판결을 내렸다.[20] 대체제도인 2016년 'EU-US Privacy Shield'[21] 역시 옴부즈맨(Ombudsman) 제도의 도입과 유럽시민이 미국법원에 개인정보 침해로 인한 손해배상 제소를 적극적으로 인정한 사법배상법(Judicial Redress Act) 인정 등을 하고 있지만 종합적으로는 보호수준이 높다고 판단하기는 여전히 힘들기 때문이다. 결론적으로 본다면 정치 및 경제적인 근거제시와 함께 형식적으로는 우리의 개인정보보호법이 자율규제 촉진이라는 규정을 가지고 있기에 이의 실효성 보장노력의 입증을 함과 동시에 감독기관의 실질적인 독립성 확보를 위한 권한확보가 입법개정을 통해 이뤄진다면 GDPR의 적절성 인증확보는 수월할 것이다. 더불어 행동강령 및 규제적 자율규제 영역에서 상대적으로 우월한 GDPR의 보호수준의 수용을 우리 제도로 수용하면 되기에 이러한 시도를 부정적인 시각으로 볼 필요는 없다.

III. 개인정보의 개념

1. 규정

개인정보의 개념은 포괄적으로 설정을 해야 기술의 발전에 따른 입법의 흠

19) 이에 대해서는 Büllesbach/Höss-Löw, Vertragslösung, Safe-Harbor oder Privacy Code oder Conduct – Handlungsoptionen globaler Unternehmen, DuD 2001, S. 135.; Klug, Persönlichkeitsschutz beim Datentransfer in die USA – Die Safe-Harbor-Lösung, RDV 2000, S. 212; 그 진행과정에 대해서는 http://www.europa-v-facebook.org 참조.

20) Judgment in Case C-362/14 Maxmillian Schrems vs Data Protection Commissioner(In der Rechtssache C 362/14 Maximillian Schrems gegen Data Protection Commissioner); 이에 대해서는 권혁심, "유럽사법재판소의 safe harbor 무효판결의 의미", 고려대 법학연구원, 고려법학 제81호, 2016.6., 77-121쪽; 문재완, "유럽연합 개인정보보호법의 특징과 최근발전", 외법논집 제40권 제1호, 2016.2., 24-48쪽; 임규철, "유럽사법재판소의 'Safe-Harbor-Principal'의 무효 판결과 그 영향", 미국헌법학회, 미국헌법연구 제26권 제3호, 2015, 121-138쪽; 이은우, "유럽사법재판소의 미국-EU 정보공유협정 무효화의 의미", 정보인권연구소 토론회, 2015.10., 1-17쪽.

21) 이에 대해서는 http://europa.eu/rapid/press-release_MEMO-16-434_en.htm 참조.

결을 최소화할 수가 있다. 또한 식별가능성이라는 판단기준에 해당 개인정보처리자 외에 제3의 개인정보처리자의 처리수준도 포함시키는 것이 정보주체에 대한 실질적인 보호가 될 수가 있다.

GDPR 제4조 제1항은 개인정보를 '식별되거나 식별가능한 정보주체와 관련된 모든 정보'라고 규정하고 있다. 해당 개인의 나이, 국적(외국인), 거주지 등은 묻지 않는다.[22] 새롭게 후단부분에 '식별가능한 정보주체는 직접 혹은 간접적으로 특히 이름, 식별번호, 위치정보, 온라인 식별자로 알아볼 수 있거나 하나 또는 그 이상의 구체적인 요소를 통하여 정보주체의 신체적, 생리적, 경제적, 문화적, 사회적 정체성이 식별될 수 있는 자'를 추가하고 있다. 따라서 GDPR에 따르면 이름, 이메일이나 전화번호 혹은 IP주소는 개인정보성이 인정되며 단서조항을 통해 기술발전에 따른 추가적인 포섭도 가능하다. GDPR 제87조에 따라 국가식별번호도 개인정보이고 그러한 정보처리는 적절한 안전조치가 있는 경우에 한해서만 활용이 가능하다.[23] 반면에 일본은 제2조 제1항 제1호에서 '개인식별번호'를 개인정보에서 명문으로 제외하고 있다. 2018 BDSG는 유럽연합의 GDPR에서 정의하고 있는 개인정보의 개념을 제량입법임에도 불구하고 별도로 국내법에서 명문으로 정의하지 않고 그대로 수용하고 있다.

우리의 개인정보보호법은 개인정보를 제2조 제1호에서 "개인정보란 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 포함)를 말한다."로 규정하고 있다.

2. 개선방향

민법상의 담보물권법 및 계약법상 물권 및 계약의 법적 개념 혹은 형사법상에 있어 폭행 및 상해의 법적 개념이 상당히 중요하듯이 개인정보법제에 있어

---

22) BVerfGE 30, 173(194); Bergmann/Möhrle/Herb, BDSG, § 3 Rn. 5.

23) GDPR 제87조(회원국은 국가마다의 식별번호나 일반적으로 적용되는 기타 식별자의 처리에 대해 구체적인 조건을 추가로 결정할 수 있다. 그 같은 경우 국가마다의 식별번호나 일반적으로 적용되는 기타 식별자는 본 규정에 따른 정보주체의 권리 및 자유를 위한 적절한 안전조치가 있는 경우에 한해서만 활용되어야 한다.).

용어에 대한 법적 개념 규정은 중요하다. 다만 법규성에 있어 논란이 있는 행정규칙을 통한 개념의 법제화는 억제할 필요가 있다. '법규로부터의 도피'이라는 행정규칙에 대한 비판은 옳다고 보기 때문이다. 물론 'RCS 해킹프로그램'이 통신비밀보호법상의 감청설비에 포함되느냐의 논란[24]이 생기면서 프로그램도 설비개념에 포함되도록 하자는 해석론 혹은 입법론처럼 기술의 발전이 법보다 앞서나가는 것이 개인정보법제에서는 극히 자연스런 현상이기에 지속적으로 추가적인 개정도 필수적이다. 더불어 과학기술법제의 일환인 개인정보보호법상의 관련 개념들에 대해서는 유연성이 보장된 포괄적 개념의 설정을 통해 법과 현실의 괴리를 줄일 수가 있어야 한다.[25]

GDPR 제4조 정의(개념)부분에서는 개인정보, 개인정보의 처리, 프로파일링, 가명처리, 파일링시스템, 개인정보처리자 및 수탁처리자, 제3자, 동의, 유출, 유전자정보 및 생체정보, 건강정보, 규제적 자율규제, 감독기관 등 26개의 개념을 법률로 정의하고 있다. 반면에 2018 BDSG는 현행 BDSG와 달리 개인정보보호법에서 독자적인 개념정의를 하지 않고 EU의 개념을 차용하고 있다.[26] 2018 BDSG의 이러한 입법방법은 입법적으로 효율적이면서 일반법의 역할을 충실히 수행하는 순기능이 있다. 반면에 국내 관련 법제에서는 정보통신망법, 신용정보법 혹은 클라우드법 등 개별법 영역에서 동일 혹은 유사한 개념들이 다르게 사용되고 있다. 개인정보보호법은 제2조에서 개인정보 및 처리의 개념을 시작으로 개인정보영상처리기기 등 7개의 법적 개념을, 표준지침으로 제3자 및 제공 등의 개념을 정의하고 있다.

GDPR 전문 제30번은 'IP주소, 온라인상의 쿠키 및 즐겨찾기' 등은 다른 정보와의 결합을 통해 명백하게 인식이 되고 제3의 서버에 의해서도 이용될 가

24) 통신비밀보호법 제2조 8. "감청설비"라 함은 대화 또는 전기통신의 감청에 사용될 수 있는 전자장치·기계장치 기타 설비를 말한다. 다만, 전기통신 기기·기구 또는 그 부품으로서 일반적으로 사용되는 것 및 청각교정을 위한 보청기 또는 이와 유사한 용도로 일반적으로 사용되는 것 중에서 대통령령이 정하는 것은 제외한다.

25) 전경운, "기술법의 발전과 향후의 연구과제", 명지대학교 기술법연구센터 제1회 학술발표대회, 2010.11., 1-13쪽.

26) 현행 BDSG는 개인정보의 처리단계를 '수집, 이용, 생산 및 폐기'로 구분하고 있다. 반면에 유럽연합의 95/46/EU에서는 처리단계를 '처리'(processing/Verarbeitung)라는 통일적인 개념으로 정의를 하고 있다. GDPR은 제4조에서 종전의 95/46/EU의 방식을 그대로 유지 및 확장을 했지만 2018 BDSG는 기존의 입법형식을 완전히 바꾸면서 GDPR의 입장을 그대로 따르고 있다.

능성을 적극적으로 경고하고 있다. 개인정보성을 인정하고 있는 것이다. 전문 제26번에서는 정보주체에 대한 식별가능성을 결정하기 위한 기준의 판단자에 대해 '개인정보처리자 또는 제3자가 정보주체의 식별성 혹은 식별가능성 확정을 위해 일반적인 기준에 따라 사용할 개연성이 큰 모든 수단을 고려해야 한다.'고 규정하고 있다.[27] 이는 '식별가능성'에 관한 기준은 유동성이지만 합리적인 범위 내에서 상당 부분 예측이 가능하기에 개인정보자기결정권의 제한사유인 명확성 원칙에 반하다고 보기는 힘들고, 판단 시 추상적으로 판단해서는 안 되고 개개의 구체적 상황에 비추어 객관적 비용이나 이해관계, 식별목적 및 보존기간 등 '종합적'으로 판단할 필요가 있다는 것으로 읽힌다.[28][29] 그 유동성은 기술의 발달에 따라 커질 수가 있기에 법과 현실의 괴리를 조금이라도 줄이기 위해 입법적으로 GDPR '식별가능한 정보주체는 직접 혹은 간접적으로 특히 이름, 식별번호, 위치정보, 온라인 식별자로 알아볼 수 있거나 하나 또는 그 이상의 구체적인 요소를 통하여 정보주체의 신체적, 생리적, 경제적, 문화적, 사회적 정체성이 식별될 수 있는 자'의 개념을 적극적으로 수용할 필요가 있다. 빅 데이터 시대에 맞는 활용이 필요하다면 적용의 일부 면제 혹은 한시적 적용면제 등의 입법을 고려하는 것이 낫지 처음부터 개인정보성을 부인할 필요는 없다. 올바른 입법태도라고 본다.

현행 BDSG 제46조 제2항에서 '업무처리상 비본질적인 초안과 메모'는 개인정보보호법 적용을 배제하고 있었지만 GDPR 및 2018 BDSG는 규정을 하고 있지 않다. 국내 법원에서는 대통령기록물관리법상 '초안 및 메모'는 본 내용이 작성되는 과정의 일환이기에 완성물이 존재한다면 해당 법에서 보존하는 기록물에 해당하지 않는다는 입장을 보이고 있다.[30] 논란이 있겠지만 초안 및 메모는 그 완성물과의 밀접한 관련성을 중심으로 개인정보성 유무가 결정된다고 볼 수가 있기에 비본질적이거나 밀접한 관련성이 없다면 개인정보성은 없다고

27) Erwägungsgrund (26) 95/46/EU도 동일한 입장이다.
28) 권건보, 「개인정보의 보호와 자기정보통제권」, 경인문화사, 2005, 13쪽; 서울중앙지법 2007.2.8. 선고 2006가합33062 · 53332 판결.
29) 개인정보보호법상의 '쉽게'라는 개념은 '합리성'(GDPR 제23조)이라고도 한다. '쉽게'의 의미는 '현실적 혹은 이론적으로 해당 정보가 다른 정보가 특별한 어려움이 없이 결합하여 특정 개인을 알아볼 수 있게 하는 것'을 말한다. 사용된 시점에서 '식별가능성을 위한 시간, 노력, 비용 등'이 그 객관적인 기준이 되기에 식별을 위한 개인정보처리자의 과다한 노력 혹은 비용이 들어간다면 개인정보성은 부인된다.; Erwägungsgrund (26) 2016/679/EU; Art. 29-Datenschutzgruppe, Personenbezogene Daten, S. 15-17.
30) 서울중앙지법 2015.3.15. 선고 2013고합1232 판결('대통령기록물 초본 누락 사건').

볼 수가 있다. 명확성을 위해 입법화도 바람직하다. 행정안전부의 해설서는 '일회성 메모나 문서작성 행위는 개인정보의 처리라고 볼 수 없다.'는 판단을 하고 있다.[31]

우리의 개인정보보호법은 개인정보의 개념을 '생존하는 개인'이라고 규정하고 있다. 따라서 '사자'(死者)의 정보는 우리의 개인정보보호법에서는 보호되는 개인정보가 아니다. 그러나 사자도 제한된 범위에서나마 인간으로서의 존엄권 역시 헌법 제10조에 의해 보호되기 때문에[32] 의료법, 통계법, 세법, 주민등록법 및 형법 등에서 사자의 개인정보에 대한 보호를 인정하고 있다. 유럽연합의 GDPR은 전문 제27번에서 해당 GDPR은 사자에게는 적용이 없지만 각 회원국들은 입법재량으로 사자의 개인정보 처리에 관한 규정을 둘 수가 있다고 규정하고 있다. 2018 BDSG은 연방법에 규정이 없기에 각 주법에 따라 해결이 될 것이다. 망자에 대한 법익이 다른 법에서 보호가 되기에 개인정보보호법의 개정을 통해 새롭게 추가적으로 보호될 이익이 있다고는 보기가 힘들다.

'법인과 단체정보'의 개념에 대해서는 개인정보보호법에 규정은 없다. 부정경쟁방지 및 영업비밀보호법에 따르면 법인과 단체정보는 '상호, 영업소재지, 대표이사 또는 대표자의 성명, 임원정보, 자산정보, 영업실적 등에 관한 일체의 정보'를 말한다. GDPR은 전문 제14번에서 '법인과 법인으로 설립된 사업체의 개인정보인 이름, 법인의 형태, 법인의 연락처 등의 처리는 이 법의 개인정보보호에 포함되지 않는다.'고 규정하고 있어 '법인과 단체정보'는 GDPR의 적용배제 대상이다.[33] 2018 BDSG도 예전과 동일하게 그러한 관련 규정이 없다. 우리의 개인정보보호법은 개인정보의 개념을 '생존 개인'으로 한정하면서 법인 및 단체정보 등을 명문적으로 배제하고 있다. 입법자의 적극적인 의사이기에 존중할 필요가 있지만 '1인 회사'의 법인 및 단체정보는 해당 기업의 영업비밀 인정 외에도 개인정보성 인정이 가능하다.[34]

---

31) 행정자치부, 「개인정보보호 법령 및 지침 · 고시 해설」, 2016.12., 17쪽.
32) 인하대학교 산학협력단,「개인정보의 범위에 관한 연구」, 개인정보보호위원회 연구보고서, 2014.10., 17쪽; BVerfGE 30, 173(194) – Mephisto 판결 –.
33) 유럽연합과 영국은 중립적인 반면 오스트리아, 스위스, 노르웨이, 덴마크, 룩셈부룩에서는 법인정보도 개인정보에 속한다고 관련 개인정보법제에서 규정하고 있었다.; 영국의 Data Protection Act 1998; Art. 2 lit. a 95/46/EU 및 오스트리아, § 4 Z 1 현행 BDSG); 스위스 Art. 3 Bst. a BDSG).
34) BGH NJW 1986, S. 2505.

Ⅳ. 개인정보처리자

1. 규정

개인정보처리자의 개념설정 시 실질적으로 개인정보롤 처리하는 자를 그 대상으로 할 필요가 있으며 가정과 관련된 개인적인 정보처리 등은 개인정보보호법제의 비적용으로 하는 입법이 효율성이 더 클 수가 있다.

GDPR 제4조 제7호에서는 개인정보처리자(controller/Verantwortliche)를 '단독으로 혹은 타인과 공동으로 개인정보의 처리의 목적 및 수단을 결정하는 자연인, 법인, 관청, 영조물 또는 다른 기관을 말한다. 개인정보의 처리의 목적 및 수단이 유럽연합법이나 회원국법에 의해 결정되는 경우에 개인정보처리자의 임명에 대한 특정한 기준을 규정할 수가 있다.'고 규정하고 있다. 민간에게도 적용되는 일반법이라는 것을 선언하고 있으며 입법재량 규정이다. 현행 BDSG는 개인정보처리자의 개념에 수탁처리자를 포함한 개념이였지만 2018 BDSG는 별도의 개념규정을 하지 않는 방식을 취했기 때문에 GDPR의 개념이 그대로 수용이 되면서 독일 법제도 개인정보처리자와 수탁처리자를 별도로 구분하여 운영이 된다.

우리의 개인정보보호법 제2조 제5호는 개인정보처리자를 "업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다."고 규정을 하고 있다. 개인정보취급자 및 수탁처리자는 별도의 규정에 의하고 있다.

2. 개선방향

개인정보보호법제의 주요 적용대상자는 국가를 막론하고 정보통신서비스사업자를 포함한 개인정보처리자이다. 그러나 개인정보의 보호 및 활용의 균형점을 달리 볼 수가 있어 이에 대한 개념정의는 각 국마다 다를 수가 있다. 일본은 제2조 제5항에서 '사업용으로 이용하는 자'를 개인정보취급자로 규정하면서 제한적으로 운영하고 있다. 이의 영향을 받아 국내 법제도 공공 및 민간영역에의 과도한 간섭배제를 이유로 개념의 정의부터 '업무목적 및 개인정보 파일'이

라는 까다로운 조건을 붙여 개인정보보호법의 적용대상을 줄이려는 입법태도를 보이고 있다. 반면에 유럽연합은 개인정보처리자의 개념을 포괄적으로 잡으면서 사적인 일이나 가정 혹은 제58조를 통해 학술연구 및 통계목적 등의 처리는 적용을 완전 혹은 일부 배제하는 입법태도를 보이고 있다. 공통적으로는 정보사회에 있어 개인정보의 활용은 필수이기에 합리적인 범위 내에서 정보주체의 동의가 없이 처리가 필요한 영역의 인정을 적극적으로 하려 한다는 점이다. 헌법재판소나 대법원의 개인정보자기결정권의 포괄성 인정이 옳다면 우선적으로는 개인정보처리자의 개념을 포괄적으로 설정하면서 유럽연합처럼 법률을 통해 적용배제 혹은 적용완화를 하는 입법방향이 좀 더 헌법친화적인 입법형식이다.

국내 개인정보처리자의 조건에 '업무목적 및 개인정보파일의 운영과 처리'가 들어가 있다. '업무'는 그 범위설정의 곤란성 때문에 논란이 많은 형법상의 업무방해죄에서 차용을 했지만[35] 개인정보보호법상의 그 범위는 형법과 달리 주된 혹은 부수적 업무와 영리 혹은 비영리업무, 보호가치 유무, 일시적 혹은 지속적 유무를 구별하지 않는다. '개인정보파일'은 쉬운 검색성, 체계성 및 집합성을 요구하고 있다.[36] '처리'는 제2조 제2호에 따라 '개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그밖에 이와 유사한 행위'를 말한다. '이와 유사한 행위'를 해설서는 '삭제, 열람, 전송 및 전달, 이전, 공유 등'을 말한다고 설명하고 있다.[37] 그 외에 '연계' 등도 가능하다. 또한 동 법은 개인정보보호법 제15조-제18조까지에서 처리단계별 규제방식에 따라 수집, 이용, 제공, 폐기 등으로 상세하게 구분하고 안전성 조치를 달리 취급하고 있다. 독일의 현행 BDSG도 제2조부터 제4a까지에서 수집, 이용, 생산 및 폐기 등을 구분하고 있었으나, 2018 BDSG는 95/46/EU 및 GDPR 제4조 제2항처럼 '처리'(processing/verarbeitung)로 단일화된 개념을 사용하고 있다. GDPR 제4조 제2항은 자동화된 혹은 비자동화된 처리를 포함하는 포괄적인 단일화된 개념을 사용하고 있다. 즉, 처리라는 개념을 '자동화된 절차에 상관이 없이 수집, 기록, 편성 및 구성, 저장, 편집, 변경, 열람, 검색, 이용, 전송을 통한 공개, 배포, 준비의 다른 형태, 비교, 연결, 제한(저장정보의 표시), 삭제 혹은 파기와 그밖에 가능한 모든 별개 혹은 일련

35) 행정자치부, 「개인정보보호 법령 및 지침 · 고시 해설」, 2016.12., 16쪽.
36) 행정자치부, 앞의 책, 15쪽.
37) 행정자치부, 앞의 책, 13쪽.

의 작업을 말한다.'고 규정하고 있다. 우리의 '이와 유사한 행위'와 같은 규정이다. 처리단계에 따라 위험성이 크게 상이하다고 보기는 어렵기에 합리적으로 보인다.[38] 이는 강제규정이다. 형사사법규정인 2018 BDSG 제46조 제7호에서도 개인정보처리자를 '개인정보처리자는 단독으로 혹은 타인과 공동으로 개인정보의 처리의 목적 및 수단을 결정하는 자연인, 법인, 관청, 영조물 또는 다른 기관을 말한다.'고 의미의 변화가 없이 그대로 규정하고 있다. 처리개념의 보호범위는 정보통신기술의 발달과 맥을 같이 하는 유연성을 가지고 있어야 하고, 수범자의 이해도를 높여 법적 안정성을 유지하자고 한다면 '업무 및 개인정보파일'을 삭제하면서 단순한 개념규정이 더 효율성이 있다. 유럽연합의 '목적과 수단을 결정하는'이라는 조건도 각 회원국에 따라 달리 판단될 수도 있기에 바람직하다고는 보기가 힘들다. 개인정보처리자를 단순하게 '개인정보를 처리하는 자'로 규정하고 예외규정을 통해 균형을 잡는 것이 입법의 효율성 및 신뢰도 증진의 방향에서는 좋다.

개인정보보호법의 적용대상은 개인정보처리자이지만 제59조에 의해 '개인정보를 처리하거나 처리하였던 자'도 처벌의 대상이 된다. 즉, 개인정보를 처리하거나 처리하였던 자가 '거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위, 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위 또는 정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 훼손·멸실·변경·위조 또는 유출하는 행위'를 하는 경우는 처벌된다. 하급심은 제71조 제5호 및 제59조의 '개인정보를 처리하거나 처리하였던 자'를 법 제2조 제5호의 '개인정보처리자'라고는 볼 수가 없다는 입장이다.[39] 아직 미공개의 판례이기에 그 판단근거를 알 수가 없지만 제59조는 제8장에 규정이 되어 있어 제58조 제1항에 따른 적용배제 영역에 있던 자도 적용이 되기에 피해자 구제확대에는 도움이 되는 판결이다.

---

38) 동일한 의견으로 최경진, 「4차산업혁명·EU GDPR 대응 개인정보보호 세미나 개최결과 종합자료집」, 개인정보보호위원회, 2017.11., 23쪽.

39) 서울서부지법 2015.12.18. 선고 2015고정1144 판결.

V. 익명정보 및 가명정보

1. 규정

빅 데이터 및 클라우드 시대는 개인정보의 처리를 전제로 하고 있어 어느 정도의 개인정보의 활용은 법적으로 보장할 필요가 있다. 비식별화로 움직이고 있는 미국과는 달리 유럽연합은 익명 및 가명정보라는 개념을 이용해 익명정보는 재식별화가 없기에 개인정보성을 부인하지만 가명정보는 추가적인 정보의 보호를 전제로 상당 범위에서 그 활용을 인정하고자 하다. 우리의 법제에서는 없는 개념들이다.

GDPR 전문 26번에서는 95/46/EU에서는 규정이 없었지만 익명정보는 원본정보에다가 식별성 혹은 식별가능성이 없도록 만든 추가적으로 처리된 정보이기에 그 개인정보성은 부인된다고 규정하고 있다. 즉, '... 익명정보에는 개인정보보호원칙이 적용되지 않는다. 이 원칙은 식별되었거나 또는 식별될 수 있는 정보주체와 관련되지 않은 정보 또는 그런 방식으로 익명처리되어 더 이상 식별될 수 없는 정보주체에는 적용되지 않는다. 이 법은 통계 및 연구목적 등을 위한 익명정보의 처리에는 적용되지 않는다.'고 규정하고 있다. 이를 통해 익명처리를 '더 이상 식별이 불가능한 추가처리'로 이해하고 있다는 것을 알 수가 있다.[40] 대체폐지가 될 95/46/EU 전문 제26번에서도 명문으로 익명정보라고 하고 있지는 않지만 '정보주체에 대해 더 이상 식별가능성이 없다면 개인정보성은 없다.'고 규정을 하고 있다. GDPR 본문 조항에서는 익명정보와 관련된 직접적인 규정이 없다. 다만 GDPR 본문 제5조 제1항 (b)에서 공공기록물 보존, 과학·역사연구 혹은 통계에 있어 목적범위 내에서 가명처리를 한 경우 보안조치 등을 행한 후 동의가 없이 제공 등이 가능하고, 제6조 제4항에서 가명처리된 정보의 경우 보안조치 등의 선행 후 처음의 목적과 연관성, 수집배경, 개인정보의 성격, 추가처리의 결과 등을 종합적으로 고려하여 동의가 없이 처리가능하다고 규정하고 있을 뿐이다. 현행 BDSG 제3조 제6항에서는 익명정보를 '시간, 노력 및 노동력의 비합리적인 현저한 비용을 통해서만 식별 혹은 식별가능성이 있는 개인정보의 수정'이라고 규정하고 있지만, 2018 BDSG에서는 해당 내용은 GDPR과 상치되기에 독자적인 익명정보의 개념을 삭제하고 유럽

40) WP-29 Opinion 05/29.

연합의 익명정보 그 개념 자체를 그대로 수용하고 있다. 이를 통해 익명정보는 식별성 및 식별가능성이 없어 개인정보성이 부인되기에 개인정보법제를 다루는 GDPR의 본문에는 규정을 하지 않았다고 볼 수가 있다. 그러나 논란불식을 위해 전문에 규정을 했다고 볼 수가 있다.

가명정보에 대해 GDPR 전문 제26번에서는 가명정보는 '추가정보를 이용하여 정보주체를 식별할 수가 있는 정보로서 식별할 수 있는 정보로 간주된다.'고 규정하고 있다. 처음으로 입법화가 된 개념이다. 가명처리의 장점으로 전문 제28번에서는 가명정보의 처리를 통해 정보주체 위험의 감소와 개인정보처리자 혹은 수탁처리자의 법 준수부담의 경감을 가져올 수가 있다고 즉, '개인정보의 가명처리는 해당 정보주체가 갖는 위험성을 줄일 수가 있으며 개인정보처리자가 그들의 개인정보보호의 의무를 준수할 수 있도록 돕는다.'고 규정하고 있다. 그렇다고 하여 가명정보의 GDPR의 배제는 아니라고 단서조항에서 규정을 하고 있다. 즉, 다른 보호대책이 없어도 이 자체만으로 개인정보처리자의 준수의무 충족으로 인정할런지는 부정확하다는 의미로 읽힌다. 전문 29번에서도 이러한 정보의 활용을 하고자 하는 경우 사전에 개인정보처리자는 보안이나 행동강령 등 그에 필요한 조직적이고 기술적인 대책(privacy be design and default 등)을 수립해야 한다고 규정하고 있다. 형사사법지침 제46조 제5호에서도 가명정보에 있어 정부주체를 알 수 있게 하는 추가적인 정보의 특별보존 및 특별한 대책마련의 필요성을 재차 강조하고 있다. 이는 가명처리가 예를 들어 보안사고 시 개인정보처리자의 면책을 위한 적절한 혹은 충분한 보장의 필요조건이 될 수는 있겠지만 필요충분조건의 충족이라고 보기는 힘들다는 의미로 읽힌다.

국내 개인정보보호법은 처음부터 익명 및 가명정보에 대한 별도의 개념규정은 없다. 다만 제3조 제7항에서 '개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.'고 규정하고 있고, 제18조 제4호에 따라 '통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우'에는 목적 외 이용 및 제공이 가능하다고 규정된 조항에서 익명처리를 예정하고 있다는 것을 예상하고 있을 뿐이다.

2. 개선방향

GDPR에 따르면 '익명정보의 처리'는 개인정보를 식별가능한 정보주체와 관련되지 않거나 정보주체를 더 이상 식별할 수 없도록 처리하는 것이고, '가명정보의 처리'는 추가적인 정보가 없이는 특정 개인을 식별할 수 없도록 개인정보를 처리하는 것을 말한다. 빅 데이터 활용처리와 관련이 깊은 개인정보처리 방식이다. GDPR은 익명정보는 개인정보성을 부정하지만 가명정보의 개인정보성은 적극적으로 인정하고 있다. 가명정보의 활용에 대해 제3자 제공 등 활용 시 보안조치나 행동강령 등 일정한 요구를 규정하고 있을 뿐이다. 일본은 '익명가공정보'[41]라는 개념으로 국내는 이와 유사한 '개인정보의 비식별성 조치'로 이에 대응하고 있는 상황이다.[42] 논문의 제한된 성격상 익명가공정보는 살펴보지는 않는다.

정보통신기술의 발달로 식별비용의 감소와 동시에 정보주체의 식별성 혹은 식별가능성의 확대가능성은 익명정보라고 피해가지를 않는다. 익명처리된 기술보다 더 나은 복구성격의 기술이라면 개별성, 연결성 및 추론성 등을 통해 저렴한 비용으로 재식별화의 수월성은 시간이 지날수록 커진다는 것이 옳다면 익명정보의 개인정보성을 완전하게 부인하는 것은 문제가 된다. 특히 고유식별성이 완벽한 주민등록번호가 해킹 등을 통해 예를 들어 'Tor' 등의 dark web이나 중국에서 공공연하게 거래되는 상황이라면 더 그렇다. 따라서 빅 데이터 정보처리의 활성화를 위해 익명정보의 개인정보성을 부인한다고 하더라도 '결합' 등

41) 제2조 제9호에서 '익명가공정보'는 '특정 개인을 식별할 수 없도록 개인정보를 가공하여 얻는 개인에 관한 정보로서 해당 개인정보를 복원할 수 없도록 한 것을 말한다.'고 규정하고 있다. 익명가공정보를 생성하기 위해서는 가명처리, 총계처리, 데이터 값 삭제, 범주화, 데이터 마스킹 등과 같은 비식별화 기술이 필요하다. 익명가공정보가 처음에는 정보주체의 동의가 없어도 제3자에게 정보를 제공할 수 있다는 의미였다가 현재는 비개인정보로 목적 외 처리가 가능하다는 것으로 의미변천이 됐다. 예를 들어 온라인상에서 이용자의 surfing 등 자동화된 수집정보로부터 익명가공정보를 생성한다면 비개인정보로 관리 및 분석과 활용이 가능하다. 그러나 익명가공정보 또한 완전한 익명정보는 아니다. 일본의 개인정보보호위원회도 익명가공정보를 '개인 특정성 저감 데이터'라고도 부른다. 익명가공정보의 기준은 위원회가 결정한다. 최저한의 기준으로 성명, 식별자(ID), 주소인 시군구 이하를 삭제 및 생년월일을 년대로 치환하고 동일 데이터베이스에 포함된 다른 개인과 데이터를 바꾸도록 하며 값에 특정 값을 부가하는 대책을 시행 중이다. 특정 개인을 식별하기 위해 다른 정보와 조합하는 것을 금지하고 있다. 안전조치를 필수적으로 요구하고 있다. 제3자에게 제공 시 개인정보 항목이나 제공방법을 공표해야 한다. 인정 개인정보보호단체를 통해 공유가 가능하지만 소비자 단체의 의견청취 의무 및 지침작성 등의 노력의무가 필수적이며 이 단체는 지침신고 및 지도나 권고 등을 위원회로부터 받는다.

42) 영국의 「Anonymisation Code of Practice(ICO)」와 「The Anonimisation Decision-Making Framework(UKAN)」 참조.

을 통한 재식별화가 있다면 그 처리위험에 대한 책임을 개인정보처리자나 혹은 사회가 예를 들어 보험 등을 통해 적절하게 부담하게 하는 입법이 필요할 수도 있다. 정부도 그러한 방향으로 부작용 최소화 정책을 시행할 예정이다.[43]

빅 데이터 활성화를 위해 2016년 6월 30일 행정안전부 및 방송통신위원회 등 정부 6개 부처는 공동안으로 '개인정보 비식별화조치 가이드라인'[44]을 제정하여 비식별화를 통한 빅 데이터 처리의 합법화를 시행 중이다. 즉, 동 가이드라인은 해당 조치에 따른 개인정보는 개인정보가 아닌 것으로 '추정'하고, 재식별 시 즉시 그 정보처리의 중단 및 파기 시는 법 위반의 책임을 면제한다고 규정하고 있다. 개인정보보호법에 없는 면책규정을 가이드라인을 통해 규정하고 있는 셈이다. 동시에 공공기관은 민간의 영리목적에 도움을 주기 위한 정보제공을 공공기관이 대행할 수가 있고, 결합정보를 원정보업체에 제공하는 것도 가능하다고 규정하고 있다. 개인정보의 상업판매에 대해서는 명시적인 없지만 위 가이드라인을 근거로 실제로 공공기관에 의해 유무상으로 제공되고 있다. 이에 개인정보보호위원회에서는 '비식별'은 익명 및 가공을 포섭하는 개념으로 수범자의 혼동가능성 증대가 예상된다고 보면서 개인정보보호법에서는 익명처리 개념을 사용하고 있기에 익명 혹은 가명정보 처리로의 용어통일과 유럽연합처럼 가명정보의 처리는 활용할 수 있도록 하면서 통계 및 연구목적 등을 위한 활용의 법적 근거를 만들 것을 권고하고 있다.[45] 위 가이드라인은 상위법에 근거가 없이 정보주체의 무력화를 불러오고 있기에 문제가 된다. 서울고등법원에서는 '정보통신망법 제30조에 따른 구글의 개인정보 제3자(NSA) 제공 내역' 공개 사건에서 "비식별 정보'(이름과 주민번호 등이 빠져 그 자체로는 누구 것인지 알아볼 수 없지만 다른 정보묶음과 결합하면 개인식별이 가능)

---

43) http://www.etoday.co.kr/news/section/newsview.php?idxno=1591819(검색어: 제4차산업혁명위원회, 검색일: 2018.3.1.)

44) 국무조정실 · 행정자치부 · 방송통신위원회 · 금융위원회 · 미래창조과학부 · 보건복지부, 「개인정보 비식별 조치 가이드라인 - 비식별 조치 기준 및 지원 · 관리체계 안내」, 2016.6.; 2014년 3월 19일 방송통신위원회의 '빅 데이터 개인정보보호 가이드라인'을 제정했지만 개인정보보호위원회에서는 동 가이드라인에 대해 개인정보보호법에 부합되지 않는 내용을 포함하고 있기에 재검토를 권고하기도 했다(개인정보보호위원회 결정, 2014 의결 제16호(2014.7.30.); 김진환, "개인정보보호의 규범적 의의와 한계" - 사법영역에서의 두 가지 주요 쟁점을 중심으로 -", 저스티스 통권 제144호, 2014.10., 61쪽; 이상윤, 「빅 데이터 법제에 관한 비교법적 연구 종합보고서」, 지역법 연구 14-16-⑦-1, 한국법제연구원, 2014.10.; 성준호, "빅 데이터 환경에서 개인정보보호에 관한 법적 검토", 경상대학교 법학연구소, 법학연구 제21권 2호, 2013., 314-321쪽.

45) 개인정보보호위원회 결정 제2017-14-122호; 제2017-09-76호.

제공내역에 있어 구글은 '비식별정보'는 정보통신망법 제30조 (구)제2항(현 제5항)에서 정한 제3자 제공현황 공개대상인 개인정보에 포함되지 않는다고 주장했지만, 제2심은 비식별정보라도 하더라도 정보통신망법 제2조 제1항 제6호에서 '해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합해 알아볼 수 있는 경우에는 그 정보도 개인정보에 포함한다.'고 규정하고 있다는 점을 근거로 들어 '비식별정보도 식별가능성이 있다면 개인정보에 포함된다."고 판결을 하고 있다.[46] 사실상 위 가이드라인을 전면으로 부정하고 있다. 영국[47]이나 유럽연합처럼 용어의 혼란을 피하기 위해 개인정보보호위원회의 권고결정처럼 익명 및 가명처리로 분류를 한 후 빅 데이터 활성화 방안을 찾는 것이 좋다. 최근 정부의 제4차산업혁명위원회에서도 비식별조치 가이드라인을 폐지하고 익명 및 가명정보 개념을 통해 개인정보의 보호와 활용의 균형점을 잡겠다고 발표하고 있다.[48]

VI. 동의

1. 규정

국내외의 법제를 막론하고 정보주체의 동의는 처리의 합법성을 보장해주는 역할을 하고 있다. 문제는 동의의 형식화를 막으면서 실질적으로 자유스러운 동의의 발현을 보장해주는 법 및 정책이 필요한 시기다. 유럽연합은 과거와 달리 그 실질성을 보장해 주는 방향으로 입법개선을 하고 있다. 우리의 법제에서는 판례로 나타나는 현상이 있다.

2018 BDSG는 현행 BDSG와는 다르게 정보주체의 정보처리 시 정보주체의 동의에 대해 형사사법규정은 별도로 하고[49] 특별한 규정이 없이 GDPR의 동

---

46) 서울고법 2016.12.22. 선고 2015나2065729 판결: 서울중앙지법 2015.10.16. 선고 2014가합38116 판결.

47) 개인정보호위원회, 「영국 정보위원회(ICO) 부위원장 대담내용」, 2016.12.

48) http://www.etoday.co.kr/news/section/newsview.php?idxno=1591819(검색어: 제4차산업혁명위원회, 검색일: 2018.3.1.)

49) 형사사법규정인 제46조 제17호는 '동의는 구체적인 상황에 있어 설명 또는 그 밖의 명백하게 인정하는 행위의 형식으로 자유스러운 것이다. 그 행위는 처리상황에 대해 고지를 받고 정보주체가 이해하고 합의함으로 착오가 없는 의사표시를 말한다.'고 규정하면서 사

의제도를 수용하는 방식으로 법 개정을 했다.

GDPR에서의 동의제도의 핵심은 GDPR 제4조 제11항과 제6조 및 제7조다. GDPR 제4조 제11항은 '동의는 정보주체가 진술(구두 혹은 문서) 혹은 명백히 긍정적인 행위에 의하든 본인과 관련된 정보처리에 대한 승낙'을 말한다고 규정하고 있다. 초안에서는 모든 개인정보에 대해 명시적인 동의를 요구하고 있었으나 최종적으로는 민감정보에 대해서만 명시적 동의를 요구하고 있다. 동의는 '자유롭게, 구체적으로, 사전의 정보제공 및 모호하지 않아야 한다.'고 규정하고 있다. 따라서 사후 동의는 부정되지만 오프라인상의 묵시적(은유적) 동의는 가능하다. '명백히 긍정적인 행위'가 무엇인지에 대해서는 논란이 가능하다. 95/46/EU의 제7조는 동의에 의한 정보처리 시 '정보주체가 동의의사를 명확하게 표시한 경우'로 규정하고 있다.[50] GDPR에서 좀 더 구체화하고 있다.

GDPR 제6조 제1항 (a)에서는 개인정보 처리의 적법성의 조건 중에서 '정보주체가 하나 또는 복수의 특정한 목적을 위하여 자신의 정보처리에 동의한 경우'에는 개인정보의 처리는 그 범위 내에서 적법하다고 규정하면서 정보주체의 복수동의를 인정하고 있다. 전문 제32번에서는 정보처리 목적의 복수인 경우 각각의 동의를 받아야 한다고 설명하면서 개별적 동의도 요구하고 있다.

GDPR을 보면 구두동의 혹은 서면동의를 각각 인정하고 있다. 규정만으로는 우열을 잡기가 어렵지만 개인정보 처리 시 동의 유무에 분쟁 시 GDPR 제7조 제1항에 따라 개인정보처리자가 그 입증을 해야 하기에 현실적으로는 법적 안정성을 위해 서면으로 처리가 많아질 것이라는 예상은 합리적이다. 장차 WP-29의 가이드라인을 통해 서면으로 권유할 개연성도 높다. 반면에 전자적인 수단을 통한 동의는 필수적으로 서면동의를 요구하고 있다. GDPR 제7조 제2항은 '서면동의 시 명백하고 쉬운 언어이면서 접근의 수월성이 보장되어야 한다.'고 규정하고 있다. 제3항은 '손실이 없는 동의거절 및 철회보장과 동의

적 자치의 동의와 동일하다는 것을 명문으로 인정하고 있다.

50) 95/46/EU은 제2조 h)에서는 동의는 '정보주체가 강요없이 구체적 사안에 있어 그 내용을 인식하고 있고 자신과 관련된 정보처리가 가능하게 하도록 하는 의사표시'를 말한다고 규정하면서 동의는 '모든 의심이 없이' 행사돼야 한다고 규정하고 있다. WP 187, Stellungnahme 15/2011 zum Begriff der Einwilligung; <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf>

시와 동의거절 혹은 철회 시는 수월성의 균일성이 보장돼야 한다.'고 규정하고 있다. 목적을 포함한 구체적인 처리상황을 동의거절 및 철회보장과 함께 개인정보처리자는 정보주체에게 고지해야 하기에 상업적인 영업목적 활용 등에 있어 분쟁이 줄어들 것으로 본다.[51] 특히 미국에서 개인정보처리자가 쿠키정보의 활용을 통한 개인정보의 상업적 판매의 경우 고지의무 유무에 대해 논란이 있지만 유럽연합은 인지될 수 있는 기회제공을 넘어 상업적 판매라는 고지의무를 명확하게 사전에 동의를 구해야 한다는 해석도 가능하기에 WP-29의 가이드라인 형성을 통해 이에 대한 구체적인 판단이 나올 개연성이 크다. 동의획득 시 불필요한 정보수집의 금지도 자유로운 동의판단의 중요한 내용이기에 필수정보 및 임의정보의 구분을 통해 불필요한 정보수집을 막을 개연성이 크다. GDPR 제7조 제1항은 동의 존재 유무 시 개인정보처리자의 입증부과 책임을, 제4항은 '정보주체의 동의가 자유스러운 결정으로 이뤄졌는지의 판단은 종합적인 상황을 고려하지만 특히 급부제공을 포함하여 계약이행 시 그것과 관련이 없는 불필요한 정보처리가 동의를 조건으로 하여 처리되었는지의 상황을 고려해야 한다.'고 규정하고 있다.

우리의 개인정보보호법도 동의제도에 대해 제4조 제2항 및 제5조 제2항, 제15조 제1항과 제2항, 제16조, 제17조 제1항과 제22조에 규정하고 있다.

2. 개선방향

개인정보처리자가 정보주체의 정보를 수집, 이용, 제공 등의 처리를 하는데 있어 정보주체의 동의를 받는 것은 사적 자치의 주요 내용이기도 하다. 국내외의 개인정보법제에서 정도의 차이는 있을지언정 정보주체의 동의내용을 다루지 않는 법제는 없다. 과거나 지금이나 개인정보처리자와 정보주체사이의 힘의

51) 전문 (42) 개인정보 처리가 정보주체의 동의에 근거하는 경우 개인정보처리자는 정보주체가 처리 방식에 대해 동의를 제공하였음을 입증할 수 있어야 한다. 특히 처리되는 사안이 아닌 다른 사안에 대해 서면으로 동의하는 경우 정보주체가 어떤 정보가 어떤 범위로 제공된다는 사실을 인지할 수 있도록 보장하여야 한다. 개인정보처리자가 제공하는 사전동의서 양식은 명확하고 평이한 언어를 사용하여 이해하기 쉽고 열람이 가능하도록 하여야 하며 불공정한 용어를 포함해서는 안 된다. 동의를 고지 받기 위해서는 정보주체는 최소한 개인정보처리자의 신원과 개인정보 처리목적에 대해 인지하고 있어야 한다. 정보주체가 진심으로 동의하지 않았다거나, 자유로운 선택으로 동의하지 않았다거나 혹은 손실 없이는 동의를 거절하거나 철회할 수 없는 경우에는 해당 동의는 자유롭게 제공된 것이라고 간주되지 않는다.

불균형은 구조적인 문제가 존재하기에 유럽연합은 동의의 엄격한 조건설정을 통해 양자간의 힘의 균형을 맞추려는 노력을 95/46/EU 이후에도 하고 있다. 이러한 노력은 GDPR에도 전문을 통해 적극적으로 반영되어 있다. 그러나 공공기관의 개인정보의 재산적 혹은 행정적 가치로의 집중이나 빅 데이터 활용에 대한 요구의 적극적인 수용과 정보주체의 'privacy paradox' 현상으로 인해 동의제도의 유명무실화를 불러올 수가 있다는 것을 동의제도 규정 시 항상 유의해야 한다.[52]

GDPR 전문 제171번은 '정보처리가 지침 95/46/EC에 따른 동의를 기반으로 할 때 정보주체는 동의방식이 GDPR의 조건에 부합하는 경우 개인정보처리자가 본 GDPR의 적용일 이후에 그 같은 정보처리를 계속하도록 허락하는 동의를 다시 제공할 필요가 없다.'고 규정하면서 두 규범의 연속성을 명문으로 보장하고 있다. 전문 제32번에서는 '승낙'의 의미를 좀 더 구체화하면서 '정보주체가 구체적인 경우에 있어 사전에 내용고지를 받고 이해되어지는 상황에서의 자유스럽게 결정된 동의'를 말한다고 하면서, 인터넷상에서의 '클릭'도 가능하지만 '침묵이나 사전에 자동적으로 존재하는 개인정보 처리동의 및 부작위'는 동의로 보지 않고 있다. 이를 통해 그동안의 묵시적 동의로의 포함가능성이 제기된 '침묵과 부작위에 대한 논란'은 없을 것이다. '전자적인 방법으로 동의를 받을 시 명백한 서면의 형태 및 정보주체가 부동의 시 서비스의 불필요한 중단이 없어야 한다.'고도 규정하고 있다. 부동의 시 불필요한 서비스 중단금지의 내용에 있어 전면적이고 포괄적인 서비스 중단금지는 안 된다는 것은 이해가 되지만 '불필요한'의 범위의 논란이 가능하다. 학설 및 판례의 축적이 필요한 부분이다. 전문 제70번에서는 '직접 마케팅을 목적으로 개인정보를 처리하는 경우 정보주체는 최초 또는 추가처리와 관련 있는 지 여부와 상관없이 이러한 직접 마케팅과 관련한 범위에 해당하는 프로파일링 등 이러한 처리에 대해 언제든지 무상으로 반대할 권리를 갖는다. 이 권리는 정보주체가 명백하게 인지할 수 있도록 제공되어야 하며 다른 기타 정보와는 별도로 명백하게 제시되어야 한다.'고 규정하고 있다. '별도의 명백한 동의'가 아닌 '명백하게 인지할 수 있는 기회제공'과 함께 DM이 가능하다는 것을 전제로 하고 있다. 동의제도의 완화를 통해 정보활용 증대를 고려한 입장이다. 전문 제33번에서는 명백한 사전인식의 예외로 과학적인 연구목적에 있어 처리목적의 불명확성이 존재하는

52) 이에 대해서는 권영준, "개인정보자기결정권과 동의제도에 대한 고찰", 전남대 법학논총 제36권 제1호, 2016.3., 673-734쪽.

경우 '과학적 연구의 공인된 윤리기준에 부합된 경우 특정 연구분야에 한해' 제한적으로 동의제공이 가능하다고 규정하고 있다.

전문 제42번에서 '손실이 없는 동의거절 및 철회보장'과 전문 제43번에서 '동의가 자유롭게 제공되기 위해서는 정보주체와 개인정보처리자 간의 명백한 불균형이 존재하는 특정 상황과 같은 경우에는 동의를 합법적인 근거로 제시해서는 안 된다. 특정 상황은 특히 개인정보처리자가 공공기관이기 때문에 동의가 자유롭게 제공될 것 같지 않은 경우이다. 개별적인 사례에서 적절하다고 판단되는 경우도 있겠으나, 별개의 개인정보 처리행위에 대해 별도의 동의를 받지 않는 경우이거나 혹은 서비스 제공 등의 계약이행이 동의가 없이 이루어질 수 있음에도 불구하고 동의에 근거하여 진행되는 경우에는 해당 동의는 자유롭게 제공된 것이라고 볼 수 없다.'고 규정하면서 정보주체보다 우월성을 가지고 있는 공공기관의 경우 정보주체의 동의가 아닌 법률을 통한 처리를 지향하고 있다는 것을 알 수가 있다.

우리의 개인정보보호법도 동의제도에 대해 관련된 많은 규정이 있다. 해당 개념규정은 없지만 제4조 제2항에서는 '정보주체의 개인정보의 처리에 관한 동의 여부, 동의범위 등을 선택하고 결정할 권리'를 규정하고 있다. 제5조 제2항에서는 '정보주체의 권리를 보호하기 위하여 법령의 개선 등 필요한 시책의 마련'을 국가의 책무로 규정하고 있어 동의권의 내용규정이 국가의 의무라는 것을 알려주고 있다. 개인정보보호위원회도 제8조 제2호의 '개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항' 및 제4호의 '개인정보 보호에 관한 법령의 해석·운용에 관한 사항'과 제8조의2의 '개인정보 침해요인 평가제도'를 통해 또는 공정거래위원회도 개인정보처리방침이라는 약관규제를 통해 정보주체의 동의권의 실질화를 보장할 수가 있다.

제15조 제1항에 따라 개인정보의 수집 및 이용에 있어 개인정보처리자는 정보주체의 동의를 받아야 한다. 제2항에 따라 동의 시 '개인정보의 수집 및 이용목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용기간 및 동의를 거부할 권리가 있다는 사실과 동의거부에 따른 불이익이 있는 경우에는 그 불이익의 내용'을 사전에 고지하고 받아야 한다. 변경 시에도 동일하다. 표준지침 제6조 제2항 제1호에서는 여기서의 동의를 '사전동의'라고 규정하고 있다. 수집과 이용목적 등을 고지하고 제22조에 따른 동의방식에 의해 동의를 받기에 사

전동의라는 판단은 타당하다.[53] 대법원도 사전동의를 의미한다고 보고 있다.[54] 제16조에 따라 '개인정보처리자는 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다. 위반의 경우 과태료의 처분대상이 된다. 해설서는 정보주체의 동의를 받으면 필요 최소한 정보 이외의 정보도 수집 및 이용이 가능하지만 제공을 의무화하거나 필수적 동의사항으로 잡는 것은 안 된다고 보고 있다.[55] 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다. 법은 '개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.'고 규정하고 있다. '필요한 최소한의 정보'가 무엇인지에 대해 개인정보보호법 제22조 제7항은 최소한의 정보의 내용에 관하여 필요한 사항은 개인정보의 수집매체 등을 고려하여 대통령령으로 정한다고 규정하고 있지만 아직까지 그 구체적인 내용은 나오지 않고 있다. 정보통신망법 제23조 제3항에서 '필요한 최소한의 개인정보는 해당 서비스의 본질적 기능을 수행하기 위하여 반드시 필요한 정보'라고 규정하고 있다. 이는 제공되는 서비스마다 필수정보와 임의정보가 다르다는 것을 보여 주고 있지만 표준지침 형식을 빌려 좀 더 구체적인 내용을 밝힐 필요가 있다.

개인정보보호법에 근거를 둔 표준지침 제6조 제3항에서는 '사회통념상 동의의 의사'라는 규정을 두고 있다. 명시적인 동의가 없어도 동의가 있다는 것으로 추정한다는 의미다. 표준지침은 개인정보처리자가 정보주체로부터 '직접 명함 또는 그와 유사한 매체(명함 등)를 제공받음으로써 개인정보를 수집하는 경우' 혹은 '정보주체가 동의의사를 명확히 표시하거나 그렇지 않은 경우 명함 등을 제공하는 정황 등에 비추어 사회통념상 동의의사가 있었다고 인정되는 범위 내에서만 이용'할 수 있다고 규정하고 있다. 제4항에서는 개인정보처리자가 인터넷 홈페이지 등 공개된 매체 또는 장소('홈페이지 등')에서 개인정보를 수집하는 경우에 해당 개인정보는 본인의 개인정보를 인터넷 홈페이지 등에 게시하거나 게시하도록 허용한 정보주체의 '동의의사가 명확히 표시되거나 인

53) 동일한 의견으로서는 이창범, 앞의 책, 123쪽.
54) 대법원 2017.4.7. 선고 2016도13263 판결.
55) 행정자치부, 앞의 책, 86쪽.

터넷 홈페이지 등의 표시내용에 비추어 사회통념상 동의의사가 있었다고 인정되는 범위 내에서만 이용'할 수 있다고 규정하고 있다. '개인정보처리자'로 행위자를 한정하면서도 '제공'은 빠져있다. 제4항은 공개된 정보의 처리의 한계를 규정하고 있는 내용으로 지침보다는 규범성이 강화된 법령을 통해 규정하는 것이 법적 안정성을 위해 좋다.

제17조 제1항에 따라 공유를 포함하여 제3자에게 개인정보의 제공 시 역시 정보주체의 동의를 받아야 한다. 제3항에 따라 '개인정보를 제공받는 자, 개인정보를 제공받는 자의 개인정보 이용목적, 제공하는 개인정보의 항목, 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의거부에 따른 불이익이 있는 경우에는 그 불이익의 내용'을 사전에 알려야 한다. 이는 변동 시에도 동일하다. 금융지주회사법 제48조의2도 금융지주회사에 속한 계열사끼리 고객정보를 공유하더라도 금융회사는 해당 정보를 고객의 동의가 없이 '외부영업'에 이용할 수 없고, 제3자에 대한 정보제공 동의를 요청할 경우 포괄적 동의가 아닌 '필수적 제3자'와 '선택적 제3자'로 나눠 동의를 받아야 한다고 규정하고 있다.[56] 과거에는 금융지주사의 자회사 간 정보공유를 '경영관리 목적 외에도 마케팅 용도로도 허용'을 했었다. 방송통신위원회는 비공개된 개인정보의 상업판매는 명확하게 인지를 시킨 후 동의를 받아야 한다는 입장으로 '개인정보 수집목적을 숨기고 경품광고 등을 통한 거짓 및 과장광고 혹은 낚시성 광고로 소비자를 유인해 개인정보를 입수한 후 보험회사 등에 판매한 '열심히커뮤니케이션즈'에 대한 시정명령'을 내렸다.[57]

---

56) 금융지주회사법 제48조의2(고객정보의 제공 및 관리) ① 금융지주회사 등은 금융실명거래 및 비밀보장에 관한 법률 제4조 제1항 및 신용정보의 이용 및 보호에 관한 법률 제32조 · 제33조에도 불구하고 금융실명거래 및 비밀보장에 관한 법률 제4조에 따른 금융거래의 내용에 관한 정보 또는 자료(금융거래정보") 및 신용정보의 이용 및 보호에 관한 법률 제32조 제1항에 따른 대통령령으로 정하는 개인신용정보를 다음 각 호의 사항에 관하여 금융위원회가 정하는 방법과 절차("고객정보제공절차")에 따라 그가 속하는 금융지주회사 등에게 신용위험관리 등 '대통령령으로 정하는 내부 경영관리상 이용하게 할 목적'으로 제공할 수 있다. 1. 제공할 수 있는 정보의 범위. 2. 고객정보의 암호화 등 처리방법. 3. 고객정보의 분리보관. 4. 고객정보의 이용기간 및 이용목적. 5. 이용기간 경과 시 고객정보의 삭제. 6. 그 밖에 고객정보의 엄격한 관리를 위하여 대통령령으로 정하는 사항. 시행령 제27조의2(고객정보의 제공 및 관리) ① 법 제48조의2 제1항 및 제2항에서 "신용위험관리 등 대통령령으로 정하는 내부 경영관리"란 각각 고객에게 상품 및 서비스를 소개하거나 구매를 권유하는 업무가 아닌 업무로서 다음 각 호의 업무를 말한다. 1. 신용위험관리 등 위험관리와 내부통제. 2. 업무 및 재산상태에 대한 검사. 3. 고객분석과 상품 및 서비스의 개발. 4. 성과관리. 5. 위탁업무 수행.

57) 방송통신위원회 2012.6.14. 결정(넥슨코리아와 열심히커뮤니케이션즈의 정보통신망법 위반

대법원도 '정보통신서비스제공자가 웹사이트의 배너 및 이벤트 광고 팝업창을 통하여 개인정보 수집 항목 및 목적과 보유기간(법정 고지시항)에 대한 안내 없이 '확인'을 선택하면 동의한 것으로 간주하는 방법은 적법한 동의를 받지 않은 것'으로 판단하고 있다.[58] 또한 홈플러스 사건에서 동의 시 전단지, 홈페이지 광고와 응모권에 기재된 내용의 동의로 볼 지에 대해 '종합적인 고려를 하면서 명확성 및 개별성'을 요구하고 있다.[59] 따라서 '포괄적 및 사실적 동의' 등은 예를 들어 약관에 개인정보 수집조건이 그런 동의내용으로 규정되어 있어 개인정보 처리 시 개인정보 수집 및 이용동의와 마케팅 및 광고활용 동의를 별도가 아닌 일괄로 받는다면 개인정보보호법 등과 공정거래법에 따른 위법논란이 가능하다. 국가인권위원회는 '지문정보의 수집 및 이용 시 제15조에 따라 정보주체의 동의를 받아야 한다. 이러한 동의가 실질적인 동의가 되기 위해서는 비동의 시 대체수단도 마련돼야 한다.'는 입장이다.[60] 이는 '대체수단의 존재'가 실질적 동의의 판단기준으로 중요하다는 것을 의미한다. 그러나 대법원은 공적 인물정보의 제한된 개인정보에 대한 상업적 판매 시 묵시적 동의를 넓게 인정하고 있다.[61]

우리의 개인정보보호법상 동의를 받는 방법은 제22조에 규정되어 있다. 제22조에 따라 동의를 받을 때에는 각각의 동의사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다. 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체와의 계약체결 등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다(GDPR 제7조 제1항 동일). 시행령 제17조 제1항에서는 동의수단으로 우편, 팩스, 전화, 홈페이지 및 메일과 이에 준하는 방법으로 명시하면서 다양한 수단을 인정하고 있다. 동의를 서면(전자문서 포함)으로 받을 때에는 개인정보의 수집·이용목적, 수집·이용하려는 개인정보의 항목 등 대통령령으로 정하는 '중요한 내용'을 행정안전부령으로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하여야 한다. 개인정

사건).

58) 대법원 2016.6.28. 선고 2014두2638 판결.

59) 대법원 2017.4.7. 선고 2016도13263 판결.

60) 국가인권위원회 2015.3.2. 권고결정.

61) 동일한 의견으로는 박노형, 「4차산업혁명·EU GDPR 대응 개인정보보호 세미나 개최결과 종합자료집」, 개인정보보호위원회, 2017.11., 8쪽; 대법원 2016.8.17. 선고 2014다235080 판결.

보처리자는 정보주체에게 재화나 서비스를 '홍보하거나 판매를 권유'하기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의도 받아야 한다. 또한 개인정보처리자는 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 안 된다. 시행령 제17조 제1항에서는 그 중요한 내용이 '개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실, 처리하려는 개인정보의 항목 중 민감정보, 여권번호, 운전면허의 면허번호 및 외국인등록번호, 개인정보의 보유 및 이용기간(제공 시에는 제공받는 자의 보유 및 이용기간), 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용목적'이라는 것을 규정하고 있다. 2017년 홈플러스의 개인정보 유상판매 사건 이후 시행규칙 제4조를 통해 행정안전부령에서 정하는 방법을 좀 더 구체화하면서 '글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게 하여 알아보기 쉽게 할 것, 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것, 동의사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시할 것'을 규정하고 있다. 개정동기가 유상판매 시 정보주체를 향한 명확한 고지에 주안점에 있었기에 유상판매라는 명문상의 규정이 없어도 해당 조항은 유상판매의 적극적인 규제내용이라는 판단을 해도 무리가 없다.

GDPR이나 우리의 개인정보보호법이나 동의제도의 핵심은 자기 자신의 정보처리에 대한 정보주체의 명백한 자유로운 의사표시라고 볼 수가 있다. 그 때문에 침묵이나 부작위 혹은 사전에 자동적으로 존재하는 동의는 그러한 의사표시라고 볼 수는 없다. 상업적 광고에 대해서는 명백한 동의가 아닌 명백한 인지의 기회제공으로 두 규범은 표현하고 있지만 상업적 판매라는 것을 명시하는 것이 좋다. 정보통신망법 개정안도 그리 규정을 하고 있다.

Ⅶ. 맺으면서

GDPR이 2018년 5월 25일부터 발효된다. GDPR에서 회원국의 입법재량이 허용된 21개의 내용을 포함해서 유럽연합 회원국 중 독일이 최초로 2018

BDSG 전면적인 개정을 통해 입법완료가 됐다.

GDPR은 유럽인의 개인정보를 처리하는 제3국에도 적용이 된다. 페이스북이나 구글 외에도 유럽연합과 경제적인 교류가 확대되는 상황에서 우리의 개인정보처리자에게도 그 영향력은 작다고 볼 수가 없다. GDPR이 제3국에도 이해가 될 정도의 보호수준의 적절성이 있는 상황에서 비합리적인 차별을 당하지 않기 위해서는 GDPR 제45조에 따른 적절성 인증을 받거나 제46조의 적절한 안전성 조치 인증 혹은 제47조의 구속적 기업규칙(BCRs) 아니면 제49조에 따른 특례 인증을 받을 필요가 있다. 국내 대기업들은 GDPR 제46-47조에 대한 대비가 가능하지만 중소기업들은 그만한 능력을 갖고 있다고 보기 힘들다. 동시에 국내 법제도 역외규정의 신설을 통해 한국민의 개인정보가 국내보다 보호수준이 낮은 국가로 국외 이전되는 것을 적극적으로 막을 필요가 있다.

GDPR의 모든 조항이 국내법제보다 우수할 수는 없지만 적극적으로 수용이 가능한 내용 및 정책도 있다. 개인정보의 개념에 있어 기술의 발전을 통해 식별가능성이 높아져 법과 기술의 괴리가 생기는 것을 조금이라도 줄이기 위해 포괄적인 개념설정이 좋다. 따라서 GDPR의 '식별가능한 정보주체는 직접 혹은 간접적으로 이름, 식별번호, 위치정보, 온라인식별자로 알아볼 수 있거나 또는 그 이상의 구체적인 요소를 통하여 정보주체의 신체적, 생리적, 경제적, 문화적, 사회적 정체성이 식별될 수 있는 자'의 정의는 그대로 수용을 해도 문제가 없다. 또한 개인정보처리자의 개념에 있어 우리의 '업무성이나 개인정보 파일' 혹은 GDPR의 '.. 개인정보의 목적 및 수단을 결정하는 ...'이라는 조건은 삭제하고 단순하게 '개인정보를 처리하는 자'로 규정하면서 시대에 맞는 예외규정 도입이 입법의 효율성 및 신뢰도 증진을 위해 바람직하다.

빅 데이터 처리와 관련이 깊은 비식별화조치 가이드라인은 판례도 호의적이지 않은 상황에서 애매하고 오해의 소지가 다분하면서 복잡한 개념이기에 법률의 규정으로 익명 및 가명정보 도입 및 운영방향을 잡아 균형을 취하는 것이 법적 안정성 측면에서 확실하다. 정부도 그러한 방향으로 방향을 잡고 있다. 동의제도의 무력화를 실질적으로 막기 위해서는 감독기관의 감독강화 및 정보주체들의 인식제고가 필요한 상황에서 침묵이나 부작위 혹은 사전에 자동적으로 존재하는 처리동의는 동의가 아닌 것으로 볼 필요가 있다. 특히 GDPR 전문 43번의 '정보주체와 개인정보처리자 간에 정보처리에 있어 명백한 불균형

이 존재하는 경우 동의를 처리의 합법적인 근거로 제시해서는 안 된다. 특히 개인정보처리자가 공공기관이기 때문에 동의가 자유롭게 제공될 것 같지 않은 경우이다. 별개의 개인정보 처리행위에 대해 별도의 동의를 받지 않는 경우이거나 혹은 서비스 제공 등의 계약이행이 동의가 없이 이루어질 수 있음에도 불구하고 동의에 근거하여 진행되는 경우에는 해당 동의는 자유롭게 제공된 것이라고 볼 수 없다.'는 규정은 신선하다. 공공기관이 정보주체의 동의라는 우회를 통해 개인정보 처리가 발생할 수가 있기 때문이다. 개인정보의 상업적 판매에 대해서는 명백하고 수월하게 사전고지 및 철회권이 보장되어야 할 필요가 있다. 두 규범의 '명백히 인지할 수 있게 하는 기회제공'으로는 부족하다. 정보통신망법 개정안은 명백하게 상업적 판매의 고지를 의무화하고 있다.

[참고문헌]

김일환, “지능정보화 사회 대응 개인정보보호 세미나 - 개인정보보호 법령간 정합성 강화 방안 -”, 개인정보보호위원회, 2017.12.

김진환, “개인정보보호의 규범적 의의와 한계” - 사법영역에서의 두 가지 주요 쟁점을 중심으로 -“, 저스티스 통권 제144호, 2014.10.

권영준, “개인정보자기결정권과 동의제도에 대한 고찰”, 전남대 법학논총 제36권 제1호, 2016.3.

박노형, 「4차산업혁명ㆍEU GDPR 대응 개인정보보호 세미나 개최결과 종합자료집」, 개인 정보보호위원회, 2017.11.

“개인정보보호법과 정보통신망법의 관계 분석”, 안암법학 제41권, 안암법학회, 2013.

성준호, “빅 데이터 환경에서 개인정보보호에 관한 법적 검토”, 경상대학교 법학연구소, 법학연구 제21권 2호, 2013.

이인호, “지능정보화 사회 대응 개인정보보호 세미나 - 개인정보보호 수행체계 효율화 방안 -”, 개인정보보호위원회, 2017.12.

임규철, “정합성의 입장에서 본 개인정보보호법 제6조와 정보통신망법 제5조의 ‘다른 법률에(서) 특별한 규정’에 대한 소고”, 서울법학 제25권 제4호, 서울시립대 법학연구소, 2018.2.

오병일, “지능정보화 사회 대응 개인정보보호 세미나 - 개인정보보호 법령간 정합성 강화 방안 -; 개인정보보호위원회의 독립성과 권한강화 필요성”, 개인정보보호위원회, 2017.12.

전경운, “기술법의 발전과 향후의 연구과제”, 명지대학교 기술법연구센터 제1회 학술발표대회, 2010.11.

한은영, “유럽연합(EU), 개인정보보호(Data Protection)강화추진”, 정보통신정책연구원, 동향 제26권 제7호, 2014.

최경진, “빅데이터와 개인정보”, 성균관대 법학연구소, 성균관법학 제25권 제2호, 2013.

고학수, “개인정보보호: 규범체계에 관한 논의의 전개와 정책적 과제”, 「개인정보보호의 법과 정책」, 박영사, 2016.

권건보, 「개인정보의 보호와 자기정보통제권」, 경인문화사, 2005.

이희정, “개인정보보호법과 다른 법과의 관계 및 규제기관 사이의 관계 - 정보통신망법과의 관계를 중심으로-”, 「개인정보보호의 법과 정책」, 박영사, 2014.

임규철, 「21세기 개인정보 정책과 법」, 북포유, 2015.
함인선, 「EU 개인정보보호법」, moronie(출), 2016.
인하대학교 산학협력단, 「개인정보의 범위에 관한 연구」, 개인정보보호위원회 연구보고서, 2014.10.
행정자치부, 「개인정보보호 법령 및 지침 · 고시 해설」, 2016.12.
KISA, 「우리 기업을 위한 GDPR 안내사항」, 2016.

[Abstract]

A Study on the improvement of legislation of domestic personal data protection act through critical acceptance of GDPR and 2018 BDSG

Lim, Gyeo-Cheol*

GDPR also applys to domestic personal data controllers that provide goods or services to EU resident data subjects or monitor the actions of data subjects. Domestic personal data controllers shall not be subject to the ‘adequate safeguards’ and ‘exceptions’ could be in accordance with Article 46 or 47 and 49 of GDPR. Certification is required to reduce the burden on personal data controllers. Of course, it is clear that an independent supervisory authority should be urgently needed.

It is desirable to delete the ‘workability and personal information file’ in the concept of the personal data controllers in the Korean Personal Data Act. In the concept of personal data, the ‘identifiable data subject’ in Article 4 (1) may be directly or indirectly identified by name, identification number, location data, online identifier or through one or more specific elements, It is necessary to reflect positively the 'person' who can identify the physiological, economic, cultural, social identity. This is because, in addition to the resident registration number, there will be no further controversy regarding whether or not personal data about the mac, IP address, cookie, and favorites is. In order to maintain legal stability in the Big Data era, legislation of anonymity and pseudonym data is needed.

Consent means the consent of an information entity to process personal data related to data subject through verbal or explicit affirmative action, according to GDPR. The consent of the consent must be clearly marked, so

* Prof. Dr. Law of Uni. Dongguk

no silence or omission, or consent to the treatment automatically pre-existing, is not considered consent. Electronic consent means only written consent. In the case of promotional purposes, separate and explicit consent is required. Written consent is a clear and easy language, with access excellence as well as assurance of rejection and withdrawal. The domestic Personal Data Act imposes the obligation of notifying the personal data controllers of the necessary consent and discretionary data and notifying the consent of the court, while aiming for prior consent. When selling personal data for sale, it enforces the display of character size, color or underline through enforcement regulations. The amendment to the Information and Communications Network Act stipulates that the declaration of commercial sale is a public obligation.

Keywords : data subject, consent, written consent, anonymity and pseudonym data, the Korean Personal Data Act, GDPR