경북대학교 법학연구원『법학논고』
제61집 (2018.04) 117~148면.
Kyungpook Natl. Univ. Law Journal
Vol.61 (Apr 2018) pp.117~148.

개인정보보호법과 EU의 GDPR에서의 프라이버시 보호에 관한 연구

조 수 영*

〈국문초록〉

제4차 산업혁명 시대는 정보통신기술의 고도화로 정보가 자원이 되고 권력이 되는 시대라 할 수 있다. 그리고 개인정보는 이러한 정보의 흐름에 중요한 축으로 작용하고 있다. 그러나 개인정보는 잘만 활용한다면 정보주체의 행복추구를 위해 최상의 서비스를 제공하는 수단이 되지만, 악용될 경우, 심각한 사생활침해로 이어져 인간의 존엄성과 그 가치로움을 몰각시킬 수 있는 양날의 검과 같다는 점에서, 순기능을 최대화하고, 역기능을 최소화할 법 정책적 노력이 필요하다 하겠다.

한편, EU는 이러한 개인정보의 순기능과 역기능의 효율적 운용을 위해 법규범적 차원의 GDPR을 제정하여, 전 회원국이 2018년 5월 25일부터 이를 시행할 예정이다. 무엇보다 정보주체의 권리보호를 위해 잊힐 권리(Right to erasure; right to be forgotten), 처리제한권(Right to restrict processing), 정보이동권(Right to data portability) 등의 권리를 규정하고 있다는 점과 공공기관이나 민간업체에 한정하지 않고, 특정요건을 갖출 경우 개인정보영향평가를 받도록 의무화하고 있다는 점에서 시사하는 바가 크다.

이에 이 논문은 EU의 GDPR을 검토하고, 우리나라 현행 개인정보보호법제와 비교하여, 제4차 산업혁명 시대에 효과적으로 대응하고, 국민의 기본권인 개인정보자기결정권(개인정보자기통제권)과 알권리 등의 보호방안에 대해 고찰해 보고자 한다.

주제어 : 개인정보 보호, EU의 GDPR, 개인정보자기결정권, 알권리, 개인식별정보, 개인식별가능정보, 잊힐 권리, 정보이동권, 처리제한권, 개인정보영향평가, PIA 국제표준지침 ISO/IEC 29134

• 투고일 : 2018.03.29. / 심사일 : 2018.04.16. / 게재확정일 : 2018.04.26.

* 법학박사, 숙명여자대학교 비전임교원

Ⅰ. 서론

현대사회는 IoE[Internet of Everything]시대를 지향하며 정보의 유통과 처리를 통해 신기술의 발전과 인간생활의 편의증진을 희구(希求)하고 있다. 그리고 이러한 당면한 현실에서 개인정보[1]는 초연결사회라 일컬어지는 고도화된 정보통신사회의 중요한 축을 이루며, 그 활용성이 좋고 나쁨에 따라 나타나는 효과는 현대사회가 지향하는 바와 판이하게 다를 수 있다는 점에서 개인정보의 활용에 있어 국가 및 사회 구성원의 보다 각별한 유의가 필요함은 누구나 공감하는 바이다. 우리나라도 제4차 산업혁명시대를 대비하며, 정부와 민간기업을 중심으로 개인정보의 순기능과 역기능을 고려한 기술발전과 인권보장의 황금률을 찾는데 노력을 게을리 하지 않고 있지만, 합의점 도출이 쉽지 않아 보인다. 최근 발생한 미국의 페이스북 사건 등을 고려할 때, 개인정보의 잘못된 처리가 전도유망한 회사의 명운까지 좌지우지할 수 있다는 점에서, 기업 및 공공기관의 특정이익 추구라는 미시적 관점의 접근보다는 정보주체의 권리보장이 궁극적으로는 그 조직의 지속가능한 성장을 이뤄낼 수 있다는 거시적 관점의 개인정보보호정책 마련이 필요하다.

2016년 5월 유럽연합(이하 EU)은 EU회원국 간의 개인정보의 자유로운 유통과 처리 및 정보주체의 개인정보관련 권리 강화를 위해 「일반 개인정보 보호법(General Data Protection Regulation, 이하 GDPR)」을 제정하고, 2018년 5월 25일부터 시행할 예정이다. 그동안 EU회원국 간의 데이터 처리에 관한 개인정보 보호의 기준을 제시한 「데이터 보호 지침Data Protection Directive 95/46/EC, 이하 '데이터 보호 지침')」과는 달리, GDPR은 EU회원국에 바로 적용되는 법규범의 효력을 갖는다는 점에서, EU전역은 물론 EU와 관련된 국가나 민간업체의 개인정보보호정책에 많은 변화를 가져올 것이라 예상한다. 무엇보다 정보주체의 권리보호를 위해 잊힐 권리(Right to erasure; right to be forgotten), 처리제한권(Right to restrict processing), 정보이동권(Right to data

1) "현행 「개인정보보호법」은 제2조에서 '개인정보'라는 용어를 사용하고 있는데, '자료(資料, data, 데이터, 문화어: 데타)는 그 단어의 의미상 '수, 영상, 단어 등의 형태로 된 의미 단위'로, 보통 연구나 조사 등의 바탕이 되는 재료를 말하며, 이러한 자료를 의미 있게 정리하면 '정보'가 됨에 유의할 필요가 있다. 현재 개인정보의 영어명은 'Personal data'로 번역된다는 점을 감안할 때, '자료(data)'와 '정보(information)'는 개념 필수적으로 그 의미가 갖는 한계가 존재한다(조수영, "개인정보보호법에서의 정보주체의 동의와 기본권 보장에 관한 연구", 한국법학회, 법학연구 제18권 제1호(통권 69호) 2018.6면)"는 점에서 이에 대한 명확한 개념 재정의가 필요함은 논외로 함.

portability) 등의 권리를 규정하고 있다는 점과 공공기관이나 민간업체에 한정하지 않고, 특정요건을 갖출 경우 개인정보영향평가를 받도록 의무화하고 있다는 점에서 시사하는 바가 크다.

이 논문은 EU의 GDPR에 대해 검토하고, 프라이버시 보호 관점에서 살펴본 후, 특히 각 회원국에게 위임된 오프닝조항을 검토하고, EU회원국의 프라이버시 방향을 점검한 후 제4차 산업혁명을 대비하며, 개인정보와 정보기술의 발전이라는 두 가지 가치의 양립 가능성을 모색해 보고자 한다.

Ⅱ. EU의 GDPR과 프라이버시 보호

1. EU의 일반 개인정보 보호법(GDPR)

1) GDPR(General Data Protection Regulation의 의의

(1) 제정 배경

1990년대 중반에 EU에서 「데이터 보호 지침」이 제정되고 시행되었을 때까지만 해도 EU사회가 지금과 같이 스마트폰이나 온라인 소셜 미디어 플랫폼, 사물인터넷, 빅데이터 등의 출현으로 인터넷의 활용이 고도로 네트워크화되고 상호 연결된 초연결 세계가 구현되리라는 생각은 못했을 것이다. 그러나 만물인터넷(IoE)시대를 지향하며 발전하고 있는 현실을 고려할 때, EU 법원 및 데이터 보호기관(DPA)은 「EU 데이터 보호 지침」을 단순히 설계되지 않은 세계에 적응시켜야 하는 어려움에 봉착하게 되었다. 이러한 난제를 해결하고 EU 회원국 간의 정보의 자유로운 이동을 보장하는 동시에 개인정보주체의 권리를 강화하기 위한 해결방안을 모색하게 되었고, 4 년간의 준비와 토론 끝에 GDPR은 2016년 4월 14일 EU 의회에서 마침내 승인 되었고, 2016년 5월 4일에 유럽 연합 공식 저널에 게재되었고, 게재 20일 후인 2016년 5월 24일 발효되었으며, 2년간의 유예기간을 거쳐 2018년 5월 25일부터 EU 전역에서 시행될 예정이다. 오랜 준비기간을 거쳐 시행되는 EU의 GDPR은 「EU 데이터 보호 지침」를 대체하며, 유럽 전역의 데이터 개인 정보 보호법을 조율하여 모든 EU 시민들의 개인 정보를 보호하고, 권한을 부여받은 해당 지역의 조직이 데이터에 접근하는 방식(privacy by design 및 privacy by default 지향)을 바꿀 수

있도록 고안되었다. 무엇보다 기존의 지침에 비해, 각국의 회원국 정부가 별동의 법안을 제정하여 통과시켜야 하는 절차를 요구하지 않고 EU 회원국의 자국내 법규와 유사한 법규범적 효력을 지닌다는 점에서 GDPR이 가져올 향후 EU 회원국과 관련 국가 및 민간분야의 변화는 개인정보보호정책의 향방을 결정짓는데 중대한 변수로 작용할 것이라 예측할 수 있다.

(2) 입법목적 및 구성

앞서 살펴본 바와 같이 GDPR의 목표는 1995년 지침이 초창기 확립 된 때와 크게 다른 데이터 중심의 세계에서 모든 EU 시민을 개인 정보 및 데이터 침해로부터 보호하는 것[2]이다. 이에 따라 GDPR 제1조에서 명시한 바와 같이 개인 정보의 처리와 그러한 데이터의 자유로운 이동과 관련하여 개인을 보호하기 위해 제정되었으며, 자연인의 기본적 권리와 자유, 특히 개인 정보 보호 권리를 보호함을 목적으로 한다. 때문에 EU에서 개인 정보의 자유로운 이동은 개인 정보 처리와 관련하여 개인을 보호하기 위해 제한되거나 금지되어서는 안 된다(GDPR 제1조). 따라서 이전 「EU 데이터 보호 지침」에서 적용되었던 데이터 프라이버시의 핵심 원칙이 여전히 이 GDPR에도 적용되지만, 관련 규제 정책에 많은 변화가 제기되어 이 규정을 준수하기 위해서는 엄격한 데이터 보호 준수 체제가 필요하며, 해당 규정을 준수하지 않을 경우 최악의 경우 최대 벌금 2000만유로 또는 전 세계 매출의 4%를 벌금을 부과 받을 수도 있다는 점에서 강력한 제재를 내용으로 하고 있다.

GDPR은 본 규정과 관련한 고려사항(recitals) 173개와 총 11개의 장에 99개의 조항으로 되어있으며, 회원국에 위임하는 약 69개의 재량위임조항인 오프닝 조항(opening clauses)을 두고 있고, 그 외에도 GDPR 제29조에 근거해 WP(working party)29[3]가 내놓은 여러 권고안이 GDPR을 구체화하여 집행될 수 있도록 하는데 기여하고 있다.

---

2) https://www.eugdpr.org/the-regulation.html

3) WP29는 각 EU 회원국의 데이터 보호 기관의 대표들로 구성된 자문기구로 유럽 데이터 보호 관리자 와 유럽위원회 (European Commission)를 의미함. 집행위원회에 개인 정보 보호 권리에 영향을 미치는 회원국의 자국법에 대한 의견을 제시하거나 EU에서 개인 정보 및 프라이버시의 처리와 관련하여 개인의 보호와 관련된 문제에 대해 대중에게 권고하는 역할을 수행하고 있음.

< 표1 > GDPR의 체계와 내용

구분	제목	주요 내용
제1장 (제1조-제4조)	일반 조항 (General provisions)	목표, 물질적 적용범위, 장소적 적용 범위, 정의
제2장 (제5조-제11조)	원칙(Principles)	개인정보 처리원칙, 처리의 적법성, 동의 조건, 정보사회 서비스와 관련된 아동의 동의 조건, 특수한 개인데이터 처리, 형사상 및 범죄에 관한 개인정보 처리, 정보주체의 식별이 요구되지 않는 처리, 정보주체의 권리, 투명성 및 양식, 정보주체의 권리 행사를 위한 투명한 정보, 의사소통 및 양식, 정보의 의무 및 개인정보에 대한 권리, 정보주체로부터 개인 데이터를 수집 할 때 정보 제공 의무, 개인데이터가 정보주체로부터 수집되지 않은 경우 정보 제공 의무, 관련자의 정보에 대한 권리
제3장 (제12조-제23조)	정보주체의 권리(Rights of the data subject)	정정권, 삭제권("잊힐 권리"), 처리 제한권, 개인정보의 수정 또는 삭제 또는 처리제한과 관련된 통지의무, 데이터 이동성에 대한 권리, 프로파일링을 포함한 자동화된 의사결정 관련 권리 등, 제한
제4장 (제24조-제43조)	컨트롤러 및 프로세서(Controller and processor)	컨트롤러의 책임, 기술 설계 및 프라이버시 친화적인 프리셋을 통한 데이터 보호, 데이터 컨트롤러 용, 조합에 설립되지 않은 관리자 또는 가공업자 대표, 프로세서, 컨트롤러 또는 프로세서의 감독 하에 처리, 가공활동 목록, 감독기구와의 협력, 개인 정보의 보안, 가공 안전성, 감독기구에 대한 개인 정보 보호 위반의 통지, 개인 정보 보호의 침해에 영향을 받은 사람에 대한 통지, 데이터 보호 영향 평가 및 사전 협의, 개인정보 보호 영향 평가, 이전 협, 데이터 보호 책임자, 데이터 보호 책임자 임명, 데이터 보호 책임자의 직책, 데이터 보호 담당관의 의무, 승인된 행동 규칙 모니터링, 인증 등
제5장 (제44조-제50조)	제3국 또는 국제기구에 대한 개인 정보의 이전(Transfers of personal data to third countries or international organisations)	데이터 전송의 일반 원칙, 타당성 판단에 근거한 데이터 전송, 적절한 보증을 조건으로 하는 데이터 전송, 내부 데이터 보호 규정 준수, EU 법에 따라 불법적인 전송 또는 공개, 특정 경우의 예외, 개인 정보 보호를 위한 국제 협력 등
제6장 (제51조-제59조)	독립적인 감독 기구 (Independent supervisory authorities)	감독기구, 감독기구 설립, 감독기구 구성원의 일반사항, 관할권, 총감독기구의 권한 등
제7장 (제60조-제76조)	협력 및 일관성(Cooperation and consistency)	협력, 상호지원, 일관성 메커니즘, 위원회의 분쟁 해결, 유럽 데이터 보호위원회, 위원회의 임무 등
제8장 (제77조-제84조)	구제책, 책임 및 제재(Remedies, liability and penalties)	소송절차의 정지, 책임 및 보상권, 행정 벌금 부과 일반 사항, 제재 등

제 9 장 (제85조-제91조)	특수 처리 상황에 대한 규정 (Provisions relating to specific processing situations)	표현 및 정보의 자유와 절차, 공공문서에 대한 공적 엑세스 및 절차, 비밀 유지 의무, 교회 및 종교 단체의 기존 데이터 보호 규칙 등
제10장 (제92조-제93조)	위임법률 및 시행법률(Delegated acts and implementing acts)	위임법률, 위원회 절차 등
제11장 (제94조-제99조)	최종규정(Final provisions)	지침 95/46 / EC의 폐지, 지침 2002/58 / EC와의 관계, 이미 체결 된 계약과의 관계, 위원회 보고서, 데이터 보호에 관한 기타 연합법 검토, 발효 및 적용 등

GDPR은 개인정보(personal data)의 처리와 관련해, 컨트롤러(controller)[4]와 프로세서(processor)[5]를 제4조 제7항과 제8항에서 각각 용어정의하고 있다. 우리나라의 현행법이 개인정보처리자에 대해 규정하며, 위탁과 개인정보취급자에 대해 규정하고 있는 것과 차이가 있다. 컨트롤러는 단독으로 또는 다른 사람과 공동으로 처리의 목적과 수단을 결정[6]하는 자연인 · 법인 · 공공기관(public authority) · 에이전시(agency)[7] · 기타 단체(other body)등을 의미하며, 프로세서는 컨트롤러를 대신하여 개인 데이터를 처리하는 주체(자연인 · 법인 · 공공기관 · 에이전시 · 기타 단체 등)를 의미한다. 우리나라의 현행법상 개인정보의 처리 등에 관한 위수탁자의 관계와 유사성을 띠고 있는데, 예를 들면, 컨트롤러의 지시에 따라 프로세서가 개인정보를 처리하며, 우리나라가 위 · 수탁 관계의 설정 시 위탁계약서를 징구하도록 하고 있는 것처럼(「개인정보보호법 제26조」, 컨트롤러도 프로세서에게 구속력 있는 서면계약을 작성하여 프로세서를 지정해야 한다(GDPR 제27조)는 유사점이 있다.

---

4) 컨트롤러는 '정보처리자' 또는 '처리관리자(responsable du traitement)'로 이해할 수 있는데, 현행 「개인정보보호법」상의 '개인정보처리자'와 유사한 의미를 지님.

5) 프로세서는 "수탁처리자' 또는 '하도급관리자, 하청업자(sous-traitant)'로 이해할 수 있는데, 현행 「개인정보보호법」상의 개인정보 처리의 '수탁자(「개인정보보호법」 제26조)'와 유사한 의미를 지님.

6) 이러한 처리의 목적과 수단이 EU 또는 회원국 법률에 따라 결정되는 경우, 컨트롤러 또는 컨트롤러의 지명을 위한 특정한 기준은 EU 또는 회원국 법률에서 규정할 수 있도록 재량위임 되어 있음.

7) 행정법상의 개념으로는 "행정관청"으로 이해할 수 있으나, 법문의 특성상 공공 또는 사적 대리행위를 하는 조직이나 단체 등으로 이해할 수 있으리라 판단됨. GDPR에서 해당 조문(제4조제7항)의 agency를 프랑스어 등에서는 un service 또는 le service로 번역사용하고 있으며, 독일문에는 "einrichtung"로 번역되어 있음.

2) GDPR의 주요내용

EU의 「데이터 보호 지침」과 비교해 GDPR의 프라이버시의 규제환경에서의 주요 특징은 크게 다섯 가지로 요약할 수 있다.

첫째, 개인데이터를 처리하는 조직이 그 적용대상이 된다는 점에서 법 적용(준수)대상의 확대 또는 관할구역이 확대되었다는 것이다. 즉, GDPR 하에서는 개인정보를 처리하는 조직의 위치에 관계없이 EU에 거주하는 정보주체의 개인 데이터를 처리하는 모든 조직에 적용되기 때문에, 우리나라에 거주하며 EU의 시민을 대상으로 개인 데이터가 포함된 서비스를 실시하는 기업(회사)도 GDPR을 준수해야 한다.

둘째, 개인정보의 개념 정의가 확대되었다. EU의 「데이터 보호 지침」 제2조a는 개인정보에 대한 용어정의에서 "개인 데이터"란 식별되거나 식별 가능한 자연인("정보주체")과 관련된 모든 정보를 의미하며, 식별 가능한 사람이란 식별 번호 또는 신체적, 생리적, 정신적, 경제적, 문화적 또는 사회적 정체성과 관련된 하나 이상의 요소를 참조하여 직접 또는 간접적으로 식별 될 수 있는 사람"이라고 규정한 반면, GDPR은 "식별되거나 식별 가능한 자연 ("정보주체")과 관련된 모든 정보(식별 가능한 사람은 특히 이름, 식별 번호, 위치데이터, 온라인 식별자와 같은 식별자 또는 신체적, 생리학적, 유전적 특성에 특정한 하나 이상의 요소를 참조하여 직접적으로 또는 간접적으로 식별 될 수 있는 사람)"로 규정(GDPR 제4조제1호)하여, 기존의 지침에 포함되지 않았던 '위치데이터', '온라인 식별자', '유전정보'가 포섭되어 적용범위가 확대되게 되었다.

셋째, EU의 「데이터 보호지침」에 비해 처벌이 강화되었다. GDPR이 요구하는 사항을 준수하지 않을 경우 GDPR기구는 법규정 위반 조직에 매년 글로벌 매출액의 4% 또는 2 천만 유로(그 중 큰 금액)까지 벌금을 부과 할 수 있다는 점에서 EU의 「데이터 보호 지침」에 비해 강제력이 확대되었기에, 이를 통해 개인정보의 보호라는 실효성을 보다 폭넓게 확보할 수 있을 것으로 보인다.

넷째, 개인정보를 처리하는 조직의 정보주체로부터의 동의 시 동의방식과 조건이 강화되었다. 개인정보를 처리하는 조직(컨트롤로, 프로세서)은 개인정보의 수집 등을 위한 동의를 받을 때, 그 동의는 분명하고 다른 사항과 구별될 수 있어야하며 명백하고 평이한 언어를 사용하여 정보주체가 쉽게 이해할 수 있도록 해야 하며, 정보주체가 쉽게 접근 할 수 있는 형태로 제공되어야 한다.

다섯째, 정보주체의 권한과 권리가 강화되었다. 정보주체의 권리보호를 위해 잊힐 권리(Right to erasure; right to be forgotten), 처리에 대한 제한권(Right to restrict processing),개인 정보의 수정 또는 삭제 또는 처리 제한과 관련된 통지 의무, 데이터 이동성에 대한 권리(데이터 이동권) 등을 규정하여, 정보주체의 권리보장에 노력을 기울이고 있다.

여섯째, privacy by design/by default 개념을 구현하기 위한 노력을 한층 강화시켰다. privacy by design은 수년간 존재해온 개념이지만 GDPR 제25조, 제42조에서와 같이 GDPR의 법적인 요구 사항의 일부가 되어, '컨트롤러는 이 법규의 요구 사항을 충족시키고 정보주체의 권리를 보호하기 위해 적절한 기술적 및 조직적 조치를 효과적인 방법으로 이행해야하며(GDPR 제25조), 프로세서가 업무 수행을 위해 필요한 개인 데이터에 대한 접근을 제한할뿐만 아니라 직무 수행을 위해 절대적으로 필요한 데이터 (데이터 최소화)를 보유하고 처리하도록 요구하고 있다는 점에서, 시스템 설계 중에 프라이버시를 추가 시키는 것이 아닌, 그 전단계인 시스템 설계의 개시에서부터 프라이버시 보호를 위한 데이터 보호를 포함시켜 설계하도록 하고 있다는 점이 특징이다.

마지막으로 데이터 보호 책임자(Data protection officer, 이하 'DPO')의 지정 의무화를 들 수 있다. DPO는 조직 내에서 데이터 보호 문제의 주요 접점을 제공하는 자로, 기존 EU의 「데이터 보호지침」에서 DPO의 지정이 의무는 아니었지만, GDPR 하에서는 '(i)공공 기관, (ii)대규모의 체계적인 모니터링에 종사하는 조직 또는 (iii)민감한 개인 데이터의 대규모 처리에 종사하는 조직(제37조)의 경우에 컨트롤러나 프로세서는 DPO를 지정해야 한다. 독일의 경우 새로 개정된 「연방데이터보호법; Bundesdatenschutzgesetz; 이하 'BDSG(neu)'」에서는 컨트롤러와 프로세서가 일반적으로 개인 데이터의 자동화된 처리에 최소한 10 명이 관련된 경우 DPO를 지정하도록 의무를 강화하고 있다.[8)]

2. EU의 GDPR과 프라이버시 보호

8) BDSG(neu) §38 Datenschutzbeauftragte nichtöffentlicher Stellen "(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen." 이에 대한 자세한 설명은 opening 조항을 설명하는 제Ⅲ장에서 설명하고자 함.

1) GDPR의 프라이버시 보호

(1) 정보주체 권리보장

개인의 프라이버시 보호는 우리나라의 현행 「헌법」은 제17조에서 규정하고 있는 '사생활의 비밀과 자유'와 연계하여 살펴볼 필요가 있는데[9], 외부의 다양한 침해로부터 개인의 사생활을 보호함을 핵심으로 하는 기본권으로, 과거에는 (주로 2000년대 이전) 개인이 외부의 간섭을 받지 않고 혼자 있을 권리 내지는 개인의 사생활이 공개되지 않을 권리로 이해되었던 반면 현대에 와서는 정보통신기술의 고도화로 정보의 이동과 처리가 집단화되고 대량화됨에 따라 사생활의 침해 가능성이 농후해 지다보니 개인의 자기정보관리권(자기정보의 흐름을 제어할 수 있는 권리, 자기정보통제권)으로 이해되고 있다.[10] 이러한 측면에서 EU의 GDPR은 정보주체의 프라이버시 보호를 위해, 자기정보통제권을 강화하는 측면에서의 정보주체의 권리보장을 구현하고 있는데, GDPR 제13조부터 제22조까지에서 "정보를 제공받을 권리(right to be informed), 정보주체의 열람권(right of access by the data subject), 정정권(right of rectification), 삭제권(일명 잊힐 권리, right of erasure; right to be forgotten), 처리에 대한 제한권(right to restriction of processing), 개인정보이동권(right to data portability), 반대권(right to object), 프로파일링을 포함한 자동화된 의사결정 관련 권리(right to related to automated decision making and profiling)"[11]를 규정하고 있다.

GDPR이 프라이버시 보호를 위해 규정하고 있는 정보주체의 권리 등에 관한 사항을 정리하면, 아래의 <표3>과 같다.

---

9) 프라이버시권은 사생활의 비밀과 자유, 통신의 비밀, 인격권, 주거의 자유 등을 포함하는 보다 포괄적 개념이기에 우리나라 헌법에 규정된 사생활의 비밀과 자유를 프라이버시권과 동등한 개념으로 이해할 수는 없다는 한계가 있음.

10) 프라이버시의 보호와 관련해 살펴보면, 고전적 의미로는 주로 불법 행위에 의해 개인의 평화와 평온을 방해하는 것에 대한 개인의 불가침권인 '혼자있을 권리'로 주장되고 있으며, 19세기 후반부터 논의가 시작되어, 매스미디어 등과 관련된 개인정보라고도 하며, '개인의 사생활이 공개되지 않을 권리'로 인식되는 경우가 많음. 그러나 현대적 의미로는 정보 기술의 발전에 따라 컴퓨터에 대량의 개인 데이터를 처리 할 수 있게 됨에 따라 "자기 정보의 흐름을 제어 할 수 있는 권리 (자기 정보 통제 권한)"로 그 개념이 변화되어 이해되고 있음(芦部信喜, 『憲法 第三版』 , 岩波書店, p.117; https://ja.wikipedia.org/wiki/プライバシー; 정종섭, 『헌법학원론』, 박영사, 638-639면)

11) 행정자치부/한국인터넷진흥원, 『우리 기업을 위한 유럽 일반개인정보보호법(GDPR)』 안내서, 2017, 36면

< 표3 > GDPR에서의 정보주체 권리보장

정보주체의 권리	내용	비고
정보를 제공받을 권리 (right to be informed)	각 개인은 자신의 데이터가 어떻게 처리되고 있으며, 그 이유에 대한 정보를 얻을 권리가 있음. -동의여부의 정보 제공: 정보주체가 개인 데이터 처리와 관련된 모든 세부 사항을 이해해야 함. -제공해야 하는 개인정보: 개인정보의 처리목적과 법적 근거, 개인데이터의 수령인 및 수령방법, 보유기간, 정보주체의 권리, 컨트롤러(또는 필요시 컨트롤러)의 대리인과 DPO의 신원 및 연락처, 제3국으로의 정보이전에 관한 상세내용 및 보호방법, 프로파일링 등 자동화된 결정의 존재 및 그 결정 관련 정보 등 -방식: 제공하는 모든 정보는 간결하고, 알기 쉽고, 쉽게 접근 할 수 있어야하며 무료이며 평이한 언어로 작성되어야 함. -제공시기: 정보주체로부터 취득: 취득한 때, 정보주체이외로부터 취득: 정보 취득 후 합리적 기간 내(최대 1개월 이내)	추가적인 정보 취득 시 추가정보 제공의무 有
정보주체의 열람권 (right of access by the data subject)	각 개인은 자신의 데이터에 관한 액세스 권한이 있음. -내용: 정보주체는 컨트롤러가 실제로 개인 데이터를 처리하는지 확인할 수 있는 권리가 있으며, 이후 정보주체의 요청 시 컨트롤러는 정보주체에게 처리된 개인 데이터의 복사본을 제공해야 함. -방식: (i) 무료사본: 컨트롤러는 열람 요구에 대해 처리중인 개인 데이터의 사본을 무상 제공할 의무 有(단, 첫 번째 요청은 무료, 추가 요청에는 “합리적인 수수료"가 부과 될 수 있음.(ii) 전자방식: 정보주체가 달리 요구하지 않는 한, 데이터 사본에 대한 전자 요청은 일반적으로 사용되는 전자 형식으로 제공되어야 함(예 : .csv 및 .txt 형식이 가장 보편적 일 것으로 예상 됨) (iii) 컨트롤러는 합리적인 방법을 통해 요구자의 신원을 확인하여(정보의 불법유출 차단) 후 액세스 권한 부여 -이행시기: 과도한 지연없이 이행 (최대 1개월 이내)	※주의사항: 컨트롤러는 잠재적 요청에 대비라는 목적(유일한 목적)으로 개인정보 보관 x
정정권 (right of rectification)	정보주체는 과도한 지연없이 자신에 관한 부정확한 개인 데이터의 수정권한을 컨트롤러로부터 얻을 권리가 있음. -내용: 정보주체는 데이터 처리의 목적을 고려하여 보완진술을 제공하거나 불완전한 개인 데이터의 완전성 제고를 할 수 있는 권리가 있음. -이행시기: 과도한 지연없이 1개월 이내(정정요구가 복잡한 경우 2개월 이내 가능)	※정정요청에 따른 조치를 하지 않은 경우, 그 이유와 이의제기권리 등에 대한 안내 필요
삭제권 (잊힐 권리, right of erasure; right to be	정보주체는 관리자로부터 과도한 지연없이 자신과 관련된 개인정보의 삭제권한을 부여 받을 권리를 가지며, 컨트롤러는 다음 사유 중 하나가 적용되는 경우 과도한 지연없이 개인 정보를 지울 의무가 있음. -개인 데이터가 수집되거나 처리되는 목적과 관련하여 더	※삭세거부사유 -표현 및 정보의 자유에 관한 권리행사, 공적 업무 수행 등 법적

forgotten)	이상 필요하지 않을 경우 -정보주체가 처리에 대한 동의를 철회하는 경우(단, 당해 처리를 위한 법적 근거가 없는 경우) -제21조(1)에 의거하여 정보주체가 반대하는 경우로, 정보주체의 데이터 처리를 위한 타당한 근거가 없는 경우 -불법적으로 처리된 개인 정보 -개인 데이터는 컨트롤러가 준수해야할 연방 또는 회원국 법률의 법적 의무 준수를 위해 삭제가 필요한 경우 -제 8 조 (1)에 언급 된 아동에게 제공할 정보사회서비스 제공과 관련하여 개인 데이터가 수집된 경우 단, 제3자에게 제공한 경우, 불가능하거나 과도하지 않는 범위 내에서 그 제3자에게 정보 삭제사실을 알려야 함.	의무 이행, 공익을 위한 보건목적,공공기록 보관, 과학 및 역사적 연구 또는 통계목적, 법적 청구권행사나 방어
처리에 대한 제한권 (right to restriction of processing)	개인은 개인의 데이터와 관련하여 그 처리를 제한 할 수 있는 권리가 있음(정보주체는 데이터가 정확하지 않다고 판단되면 개인 데이터 처리를 제한 할 수 있으며, 이 경우 데이터의 정확성이 확인 될 때까지 처리를 제한해야 함.) -내용: 컨트롤러는 정보주체가 정보의 정확성에 이의를 제기하거나, 처리가 불법적이지만, 정보주체가 삭제를 반대하고 처리제한을 요구한 경우, 불필요한 개인정보에 대해 정보주체가 법적 청구권행사나 방어를 위해 해당 정보를 요구한 경우, 정보주체가 처리를 반대하였으나 컨트롤러의 정당한 사유(공익목적, 법적 의무 준수 등)가 있어 이익형량 검토를 진행하고 있는 경우 정보주체의 처리제한 요구를 이행해야 함. 단, 제3자에게 제공한 경우, 불가능하거나 과도하지 않는 범위 내에서 그 제3자에게 정보 처리제한사실을 알려야 함. -해제: 컨트롤러는 정보주체의 동의,EU회원국의 공익상 목적 등의 사유로 처리제한을 해제할 경우 정보주체에게 알려야 함.	※과도한 지연없이 그리고 수령 후 1 개월 이내에 제한 요청에 응답 할 수 있는 프로세스를 갖추고 있어야 함.
데이터이동권 (right to data portability)	개인이 서로 다른 서비스를 통해 자신의 목적을 위해 개인 데이터를 얻고 재사용 할 수있게 요구할 수 있는 권리 -내용: (ⅰ)개인이 컨트롤러에 제공 한 개인 데이터로, (ⅱ) 그 처리가 개인의 동의 또는 계약 수행에 근거한 경우이며, (ⅲ) 처리가 자동화된 수단에 의해 수행 될 때 -방식: 컨트롤러는 일반적으로 사용되는 구조화되고 기계로 판독 가능한 형태로 개인 데이터를 제공해야 함. -제한: 지적재산권이나 영업비밀 등 제3자의 권리가 침해되는 경우 이동권이 제한됨.	※기계 판독 가능: 소프트웨어가 데이터의 특정 요소를 추출 할 수 있도록 정보가 구조화되어 있음을 의미
반대권 (right to object)	개인은 개인데이터 처리와 관련해, “자신의 특정 상황과 관련된 근거"에 이의를 제기할 권리를 가짐. -내용: 개인은 컨트롤러의 정당한 이익, 공공의 이익/ 공식적 권한을 부여받은 업무수행(프로파일링 포함)에 기초한 처리, 직접 마케팅[12] (프로파일링 포함), 과학/역사 연구 및 통계의 목적을 위한 처리를 거부 할 권리[13]가 있음. -이행: 컨트롤러는 개인의 이익, 권리 및 자유 보다 더 공정하고 합법적인 근거를 입증 할 수 있거나 그 처리가 법적 청구권의 확정, 행사 또는 방어를 위한 것이 아니면	※온라인 서비스는 개인이 온라인상에서 반대하는 방법을 제시해야 함.

	정보주체의 반대권 행사에 응해야 함. -방식: 컨트롤러는 정보주체와의 최초 연락 시 반대권이 있음을 명시적으로 강조하여, 분명히 알려야 함.	
프로파일링을 포함한 자동화된 의사결정 관련 권리(right to related to automated decision making and profiling)	자동화된 의사 결정(사람의 개입 없이 자동화 된 방법으로만 결정을 내림)과 프로파일링[14](개인에 대한 특정 사항을 평가하기 위한 개인 데이터의 자동 처리)을 할 경우, 정보주체의 권리보장과 보호조치를 취해야 함. -내용: 정보주체 권리보장(인적개입요구권, 정보주체의 관점(이익)표현권, 그 결정에대한 설명요구권/반대권)과 보호조치(처리의 공정성과 투명성 보장, 프로파일링을 위한 적합한 방법 사용, 차별적 결과 방지, 오류의 시정과 실수위험 최소화 조치 등) -제한: 컨트롤러는 계약 체결 또는 이행에 필요한 경우, EU나 회원국 법률에 의해 허가된 경우, 그 결정이 개인의 명시적인 동의에 따라 이뤄진 경우 이 권리는 적용되지 아니함. -의무: 컨트롤러는 시스템이 의도한대로 작동하는지 정기적으로 확인해야 함.	※주의: 자동화된 결정은 아동과 관련성이 없어야 하며, 민감한 정보는 원칙적으로 처리가 금지됨.

(2) 데이터 보호 책임자(DPO)의 지정과 개인정보영향평가(PIA)

GDPR은 프라이버시 보호를 위해 데이터보호책임자(DPO)를 지정토록 하고 있으며, “privacy by design/ by defaul’에 따라 프라이버시 위험을 설계단계에서 검토하여 프로젝트의 데이터 보호 위험을 식별하고 최소화하는 프로세스인 DPIA (데이터 보호 영향 평가)를 특정요건에 해당할 경우 실시토록 의무화하고 있다.[15]

DPO는 대규모로 정보주체를 정기적으로 체계적으로 모니터링해야하는 데이터 처리 작업이거나 특수한 범주의 데이터(예: 건강, 종교, 인종, 성적 취향 등과 같은 민감한 데이터) 및 범죄 유죄 판결 및 범죄와 관련된 개인 데이터의 대규모 처리의 처리 시 해당 조직의 DPO지정은 필수이며[16], (ⅰ) 조직 및 직원에게 GDPR에 따른 데이터 보호 의무를 통보하고 조언하는 업무, (ⅱ) 조직의 GDPR 준수 및 내부 데이터 보호 정책 및 절차 준수 여부 모니터링 또는 책임배정 업무(인식 교육, 공정 운영 및 관련 감사와 관련된 직원 교육이 포

12) 직접 마케팅 목적으로 개인 데이터 처리를 중단해야하며, 거절할 수 있는 면제 나 근거가 없음.
13) 공익 업무 수행을 위해 개인 데이터 처리가 필요한 연구를 수행하는 경우 처리에 대한 이의를 준수할 필요가 없음.
14) 프로파일링은 자동화 된 의사 결정 프로세스의 일부가 될 수 있음.
15) DPIA에 대해서는 제Ⅱ장 2.(2)에서 후술하고자 함.
16) 앞서 언급한 바와 같이 독일은 「연방데이터보호법(BDSG)」의 개정을 통해 그 요건을 강화하고 있음.

함), (ⅲ)데이터 보호 영향 평가 (DPIA)의 필요성, 구현 방식 및 결과에 대해 조언, (ⅳ)데이터 유출보고를 포함한 모든 데이터 보호 문제에 대한 데이터 보호 기관의 연락처 역할 수행, (ⅴ)정보주체의 열람권(액세스 요청) 행사를 포함하여 개인 정보 문제에 대한 개인(정보주체)과의 접촉자 역할 등을 담당한다. DPO는 데이터보호프로그램의 구축,구현 및 관리하는 방법을 이해하는 것이 중요하며, 반드시 변호사일 필요는 없지만 GDPR과 회원국내의 관련법에 대한 심층적인 지식을 갖춘 자여야 하며, 해당 조직의 규칙과 절차에 대한 올바른 지식을 갖추고 있어야 한다. GDPR은 DPO의 업무수행 방식에 독립성을 제고토록하여, 조직의 고용주의 지시 없이 운영되도록 하고 있다. 이는 조직의 이익보다는 정보주체의 권리보장 등을 공정하고 형평성 있게 다룰 수 있다는 점에서, 보다 프라이버시 보호에 적합한 정책이라 하겠다. 한편, GDPR상의 DPO는 우리나라의 「개인정보보호법」 제31조의 '개인정보책임자'와 유사한 개념이나, 직무상 완전한 독립성이 보장되고 그 책임의 범위와 유형에 차이가 있다는 점에서, GDPR의 구현정도를 지켜보며, DPO에 대한 보다 체계적인 연구와 그에 따른 우리나라 현행법상의 개인정보책임자의 지위와 역할에 관한 장단점 비교를 통한 우리나라법체계에 맞는 개인정보보호책임자제도의 개정방안을 마련할 필요성이 있다.

2) GDPR의 DPIA와 PIA 국제 표준지침

(1) GDPR의 DPIA

GDPR 제35조에 따를 때, 조직은 새로운 처리 활동으로 인해 발생할 수 있는 잠재적 위험을 평가하기 위해 영향 평가를 수행해야 한다. DPIA는 GDPR에서의 개인정보영향평가를 의미하며, 데이터보호영향평가(Data Protection Impact Assessment; 이하 'DPIA')로 일반적으로 약어로 'DPIA' 불려진다. 한편, 개인정보영향평가(PIA)는 개인식별정보(Personally identifiable information, PII)를 처리하는 프로세스, 정보시스템, 프로그램, 소프트웨어 모듈, 장치 또는 기타 이니셔티브에 미치는 잠재적 영향을 평가하고 이해 관계자와 상의하여 필요한 개인 정보 보호 조치를 취하기 위한 도구로, 데이터 처리 대상에 대한 높은 위험도를 초래하는 새로운 처리 활동이 제안 된 경우(특히 신기술이 사용될 경우), 컨트롤러는 먼저 영향 평가를 수행해야한다. GDPR 제29조에 따른 WP29에 따르면 위험 수준을 높이는 요소에는 데이터 주체의 평가(예: 직장에서의 수행, 건강, 행동 또는 위치); 자동화된 의사결정(예: 자동거부); 체계적인

모니터링(특히 은밀한 모니터링);민감한 개인 데이터 처리;대규모 처리;별도의 데이터 세트를 결합하거나 매칭하는 것; 취약한 개인(예: 아동 등)에게 영향을 미치는 처리; 시험되지 않은 기술을 사용하여 처리; 국경 간 데이터 전송 등이 있다. 독일의 경우 2018년 5월 25일부터 시행될 개정 「독일연방데이터보호법,BDSG(neu)」제67조는 GDPR 제35조에 따라 컨트롤러에게 영향평가를 실시토록 의무화 하고 있다. 한편, PIA의 실시와 관련해, WP29는 GDPR의 WP248에서 DPIA의 방법론 제공근거:유럽 데이터 보호 당국 (WP29)은 PIA 국제표준지침(International Standard ISO/IEC 29134)이 DPIA수행에 사용되는 방법론에 대한 지침역할이 될 수 있다고 설명하고 있다.[17]

(2) PIA 국제 표준지침 ISO/IEC 29134

PIA는 국제 표준화위원회 ISO TC68 (금융 서비스 전문위원회)에서 2008 년 4 월에 ISO22307 (Financial services Privacy impact assessment)로 표준 문서가 발행되었으며, 2017년 발행된 'PIA 국제표준지침(International Standard ISO/IEC 29134)'은 일반적인 사항에 적용토록 고안되었다. ISO(국제 표준화 기구; International Organization for Standardization[18]) 및 IEC(국제 전기 표준회의;International Electrotechnical Commission[19])는 각 나라마다 다른 산업, 통상 표준의 문제점을 해결하고자 국제적으로 통용되는 표준을 개발하고 보급하기 위해 ISO/IEC Directives를 작성하여 운영 중에 있는데, 대한민국은 1963년 ISO에 회원으로 최초 가입하였으며, 현재 기술표준원(KATS: Korean Agency for Technology and Standards)이 정회원으로 활동하고 있다.[20] 'PIA 국제표준지침(International Standard ISO/IEC 29134)'은 개인정보가 처리되는 다양한 상황에 맞게 조정할 수 있는 지침을 제공하며, <표3>과 같이 구성되어 있다.

17) wp248(ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679), p.5, p.20.

18) 여러 나라의 표준 제정 단체들의 대표들로 이루어진 국제적인 표준화 기구

19) 전기 기기에 관한 국제 표준화 담당

20) 1963년 (전)공업진흥청이 ISO에 회원으로 최초 가입하였으며, 정부조직개편에 따라 1997년 국립기술품질원(KNITQ: Korean National Institute of Technology and Quality)으로 회원기관 명칭 변경 신청을 하였고, 1999년 이후로는 기술표준원(KATS: Korean Agency for Technology and Standards)이 정회원으로 활동하고 있음.

< 표4 > 'PIA 국제표준지침(International Standard ISO/IEC 29134)'의 구성

목 차	
1 범위 2 참고 문헌 3 용어 정의 4 약식 용어 5 PIA를 위한 준비 5.1 PIA 실시의 이점 5.2 PIA 보고의 목적 5.3 PIA 실시 책임 5.4 PIA 규모 6 PIA 실시 절차 6.1 일반 6.2 PIA의 필요성 판단(시작점 분석)	6.3 PIA 준비 6.4 PIA 수행 6.5 PIA 후속 조치 7 PIA 보고 7.1 일반 사항 7.2 보고 구조 7.3 PIA의 범위 7.4 프라이버시 요구 사항 7.5 위험 평가 7.6 위험 처리 계획 7.7 결론 및 결정 7.8 PIA 공개 요약

'PIA 국제표준(International Standard ISO/IEC 29134)'에 따를 때, 일반적으로 PIA는 "(i)프라이버시 영향, 프라이버시 위험 및 책임의 확인, (ii)privacy by design을 위한 경우, (iii) 새로운 정보 시스템의 프라이버시 위험성 검토 및 그 영향과 가능성 평가, (iv) 권장된 개인정보 주요완화조치에 따라 데이터 주체에 프라이버시 정보의 공급을 위한 기초제공, (v) 처리된 개인정보에 영향을 줄 수 있는 변경사항의 유지관리, (vi) 이해 관계자와 프라이버시 위험을 공유 및 완화하거나 그 준수와 관련된 증거를 제공하는 행위"[21] 등과 같은 목적으로 수행할 수 있음을 설명하고 있다. 국내법과의 비교를 통한 보다 자세한 사항의 기술은 제Ⅳ장에서 하고자 한다.

Ⅲ. GDPR상의 오프닝 조항과 프라이버시 보호

1. GDPR상의 오프닝 조항

EU의 GDPR은 회원국의 자국법에 우선하는 법적 효력을 지닌 법규범이지만, 회원국의 자국 내 상황을 무시한 일반적 법규범을 운영하는데 무리가 있을 수 있다는 판단 하에, 회원국의 자국내 상황을 고려한 재량규정을 두고 있음. 일명 개별조항(Opening Clauses)은 회원국의 자국내 법규에 따라 GDPR의 조항을 수정할 수 있게 하고 있다. 일종의 위임재량조항에 해당하는데, 필요한

21) ISO/IEC 29134:2017(E) p.4

경우 개별 조문에서 회원국이 자국 내 법규를 통해 GDPR 의무를 보다 제한적으로 적용 할 수 있게 하는 특징이 있다. 다음은 GDPR에 규정된 회원국에 허용된 개별조항(Opening Clauses)을 목록화한 것이다.

< 표5 > GDPR과 EU 회원국의 오프닝 조항(Opening Clauses)

범위	개별조항	내용	강제 여부	비 고
법적 근거에 의한 데이터 처리	제4조제7항	책임자의 역할 할당		
	제6조(1)(a) (c)	법률의 적법성. 의무		
	제6조(1)(a) (e)	공무 수행 업무의 적법성, 이해관계인 또는 공공 기관		
	제6조(4)	목적 제한 원칙의 예외		
	제9조(2)(g)	민감한 데이터의 처리에 대한 국내 법적 근거		
	제11조(5)(c)	정보 의무의 예외		
	제26조(1)	공동 책임자에 대한 업무 할당		
	제28조(3) 첫 번째 문장	법적 근거에 의한 주문 처리 (계약 대신)		
	제28조(4)	계약 대신 법적 근거에 의한 하도급		
	제35조(10)	영향평가 의무의 예외		
특별히 보호 된 데이터 처리	제9조(3)민감한 데이터 처리 목적을 위한 사항 과 관련한 제9조(2) (h)	보건의료 및 직업병 의학과 관련한 민감한 데이터 처리 가능 (회원국의 관할 기관의 규칙에 따라 전문적인 비밀 보장을 받는 경우 (2)(h)에 명시된 목적으로 처리 될 수 있음)		
	제9조(2)(i)	공중 보건 목적의 민감한 데이터 처리		
	제9조(4)	유전 적, 생체 인식 또는 건강 데이터		
	제10조	형사상 관련 데이터의 처리 금지에 대한 예외		
	제36조(5)	사전 협의 또는 가공 승인, 공중 보건을 포함한 공익		
	제49조(5)	최고의 전송에 대한 제한. 제 3 국에 대한 데이터 카테고리		
	제87조	이해관계자의 권리와 자유에 대한 적절한 안전장치를 마련한다는 조건 하에서의) 국가 색인 처리 허용		
영향을 받는 권한	제11조(5)(d)	전문 비밀 유지의 경우 정보 제공 의무의 면제		
	제17조(1)	특별 취소 의무		
	제17조(3)(b)	삭제 의무 면제		
	제22조(2)(b)	자동 의사 결정 및 프로파일링의 적합성		
	제23조	피해자의 권리에 대한 제한		

		-국가 안보, 국방, 공공 안전, 공공 안전에 대한 위협의 방지 및 방지를 포함한 형사 범죄의 예방, 조사, 탐지, 기소 또는 기소 등을 달성하는데 필요 -다른 사람의 개인이나 권리와 자유를 보호하기 위해 -민사 청구를 집행하기 위해 -형사 범죄의 예방, 조사, 탐지 또는 기소 (개인에 의한)		
동의	제8조(2)	아동의 동의 연령 제한		
	제9조(2)(a)	민감한 데이터의 처리에 대한 동의의 제한		
DPO	제37조(4)	데이터 보호 책임자 지정 의무		
계약자 프로세서	제28조(3) (a)	프로세서에 대한 데이터 처리 의무		
	제28조(3)(a)과 이에 따른 제28조(2)	책임자에게 통보 금지 프로세서별 처리		
	제 28 조 (3)(g)	프로세서의 보관 요건		
	제29조 및 제32조(4)	프로세서 및 개인 데이터에 액세스 할 수있는 컨트롤러 또는 프로세서의 대상자는 연방 또는 국가 법률에 따른 프로세서의 지침 면제		
보관 조사 목적 또는 통계 목적	제9조(2)(j)	기록 보존 목적, 과학적 또는 역사적 연구 목적 및 통계 목적의 민감한 데이터 처리를 위한 법적 근거		
	제89조(2)	역사적 연구 또는 통계 목적 과학적 자료로 가공 될 때 데이터 주체의 권리에 대한 예외		
	제89조(3)	보관 목적을 한 데이터 주체 권리에 대한 예외		
데이터 보호 기관의 설계를 위한 재량	제68조(4)와 관련한 제51조(3)	다수의 DPO 규정		대한민국 기업과는 관련성이 별로 없는 영역
	제52조(4)-(6)	감독 당국에 필요한 인적, 기술 및 재원, 시설 및 인프라가 제공되도록해야 함	강제 조항	
	제55조(3)	법원을 감독 할 특별기구 설치		
	제51조(1)와 관련한 제54조(1) (a)	DSB 및 책임 배정	강제 조항	
	제53조(3)과 관련한 제54조(1)(d)	임기		
	제54조(2)와 제53조(2)	감독 당국의 설립	강제 조항	
	제54조(1)(e)	재임명	강제 조항	
	제54조(1)(f)	직원의 의무, 비 호환성, 해지	강제 조항	
	제54조(2)	공식 비밀		

	제91조(2)	교회와 종교 단체 또는 공동체를 위한 DPO 특정		
데이터 보호 기관의 권한	제57조(1) (c)	의회와 정부에 대한 자문 서비스의 규제	강제 조항	
	제58조(1) (f)	데이터 보호 주택 검색 절차	강제 조항	
	제58조(3) (b)	비공개 기관 및 일반 대중에 대한 의견		
	제58조(4)	감독당국에 대한 절차 법 및 구제	강제 조항	
	제58조(5)	소급 권 및 감독당국의 권한		
	제58조(6)	감독당국의 추가권한		
	제59조(2)	보고서가 제출 될 당국		
	제62조(3)	공동 작업에 관여하는 감독 당국의 구성원 또는 직원에게 조사 권한의 위임 등		
	제90조(1)	전문직 비밀 보유자에 대한 권한 행사		
NGO[22] 대리행사 범위	제80조(1)	손해배상 청구에 대한 대변 가능성		
	제80조(2)	집단 행동		
벌금 및 제재	제83조(7)	공공 당국 및 공공 당국에 대한 벌금		
	제83조(8)	벌금 부과 절차	강제 조항	
	제84조	특히 제 83 조에 언급되지 않은 위반에 대한 추가 제재		
기본적인 권리충돌 해결	제85조(1)	회원국은 법령에 따라 이 규정에 따른 개인정보보호 권리를 언론보도 목적 및 과학적, 예술적 또는 문학적 목적을 위한 표현을 포함한 표현 및 정보의 자유와 조화시켜야 함		
	제85조(2)	저널리즘 목적이나 과학적, 예술적 또는 문학적 목적으로 처리하기 위해 회원국은 제2장 (원칙), 제3장 (데이터 주체의 권리), 제4장 (책임 및 프로세서), 제5장 (개인 정보의 제3국 또는 국제기구로의 이전), 제6 장(독립적감독당국), 제7장 (협력 및 일관성) 및 제9장 (특별 처리 상황을 위한 규칙) 표현의 자유와 정보의 자유가 보장됨	강제 조항	
	제86조	공식 문서에 대한 접근 허용		
고용 관계	제9조(2)(b)	가공의 법적 기반으로서의 노동 및 사회 입법 중요한 데이터		
	제88조	회원국은 법률 또는 단체 협약에 의해 부과된 의무이행을 포함하여 고용 계약의 이행, 고용을 목적으로 고용 조건에서 개인 고용 데이터 처리와 관련하여 권리와 자유를 보호하기 위한보다 구체적인 규칙을 입법이나 단체 협약을 통해 제공 할 수있음. -업무의 계획과 조직, 직장의 평등과 다양성, 직장의 건강과 안전, 고용주 또는 고객의 재산 보호, 고용, 개인 또는 집단적 권리와 이익의 사용, 그리고 고용 종료의 제공 -이 규칙은 특히 처리의 투명성, 공동의 경제 활동에 종사하는 회사 그룹 또는 기업 집단 내에서의 개인 데이터		

		의 이전과 관련하여 인간 존엄성, 합법적 이익 및 데이터 주체의 기본적 권리를 보호하기 위한 적절하고 구체적인 조치를 포함해야함(그리고 작업장의 모니터링 시스템을 포함함)		

2. GDPR상의 오프닝 조항과 프라이버시 보호

앞서 살펴본 바와 같이 총 99개의 조문 중에 약 69개의 조문이 회원국에게 일종의 자유재량을 위임하는 형식의 오프닝조항을 두고 있다. 이는 GDPR의 법규범으로서 별도의 회원국 내의 법제정 없이 발효되는 특징으로 인해, 자칫 회원국 내에서 지키고자 하는 가치와 충돌할 가능성에 대비해 재량의 범위 내에서 회원국의 법제에 맞는 GDPR을 실시토록하기 위한 것이다. 상황이 이렇다보니, 2018년 5월 25일 GDPR의 시행을 앞두고 있는 EU회원국 중 새로운 법제 정비를 통해, Opening조항을 반영한 회원국(독일)도 있고, 준비단계에 있는 회원국(예: 네덜란드[23], 라트비아[24], 룩셈부르크[25], 리투아니아[26],몰타[27], 벨기에[28], 스페인[29], 슬로바키아[30], 영국[31], 프랑스[32] 등)도 있으며, 아직 이렇다 할 준비 없이 바로 GDPR이 적용되는 회원국(예:그리스, 덴마크, 루마니아 등)도 있다.

이 중 독일의 경우 2017년 GDPR시행에 맞춰 BDSG가 개정이 되었으며, 2018년 5월 25일 GDPR과 함께 발효되면, 현행연방 데이터 보호법을 완전히 대체할 예정인데, 아래의 <표6>을 통해 확인할 수 있는 바와 같이, 무엇보다 Opening Clauses조항을 활용하여, 독일에 맞게끔 강화된 조항을 두고 있다.

---

22) 단체, 단체 및 협회를 통한 이해 관계자 대표
23) GDPR 이행 법안(Uitvoeringswet Algemene verdenening gegevensbescherming, Bill) 2017 년 12 월 13 일에 의회에 제출됨. 2018년 3월 8일 의회 본회 진행 예정
24) 법률(Personas datu apstrādes likums) 초안은 각료회의에서 검토 중
25) GDPR의 이행에 관한 “초안 법안(n 7184, 이하 “초안 법안”) 발표됨. 그러나 자국에 맞게 수정될 예정에 있음.
26) 리투아니아 공화국 법무부는 법률안을 준비 중에 있음.
27) 초안 작성 - 곧 의회 승인 진행 예정.
28) 법 초안 작성 단계 (아직 게시되지 않음)
29) 법안 진행 중
30) 의회에서 법안 초안 진행 중
31) Bill 초안 은 2016 년 9 월 14 일에 게시되었음.
32) 프랑스 2017 년 12 월 13 일에 초안을 채택. 프랑스 의회에서 검토 중

< 표6 > 독일 BDSG(개정)의 주요사항

범위	주요내용	관련 조문
데이터 보호 책임자의 지위 강화	10 명 이상의 자동화된 개인정보 처리를 담당하는 조직의 데이터 보호 책임자 임명(그외 GDPR 제35조에 따른 DPIA가 필요한 경우, 사업상의 개인 데이터의 처리로 정보주체의 자유와 권리에 위험이 발생할 경우 데이터보호책임자 임명)	BDSG 제38조
고용 데이터 처리를 위한 GDPR 제88조 처리 특례	고용 관계를 수립하거나 고용 관계를 확립하거나 법 또는 단체 교섭 협약에 따라 의무를 이행하거나 이행하기로 결정한 경우 직원의 개인 데이터를 고용 목적으로 처리 할 수 있음. 그러나 처리시 주의사항 있음.	GDPR 제88조 BDSG 제26조
새로운 데이터 보안 조치	-권한이 없는 자에 대한 처리가 수행되는 처리 설비에 대한 액세스 거부 (액세스 제어) -데이터 캐리어의 무단 읽기, 복사, 변경 또는 삭제 방지 (볼륨 컨트롤) -개인 정보의 무단 입력 및 저장된 개인 정보의 무단 지식, 수정 및 삭제 방지 (저장 장치 관리) -승인되지 않은 데이터 전송 설비 (사용자 제어)를 통한 자동 처리 시스템 사용 방지 -자동 처리 시스템을 사용할 권리가있는 사람이 자신의 액세스 권한 (액세스 제어)이 적용되는 개인 데이터에만 액세스 할 수 있도록 보장 -개인 데이터가 데이터 전송 시설 (전송 제어)을 통해 전송되거나 이용 가능하게 된 장소를 확인하고 결정할 수 있는지 확인. -자동 처리 시스템 (입력 제어)에서 언제 어떤 개인 데이터가 입력되거나 변경되었는지, 그리고 누구에 의해 확인되었는지를 확인하고 확인할 수 있음을 보장 -개인 정보의 전송 및 데이터 매체의 전송 (전송 제어)에서 데이터의 기밀성 및 무결성이 보호되는지 확인하고, -장애가 발생한 경우 사용 된 시스템을 복원 할 수 있는지 확인 (복구 가능성) -시스템의 모든 기능을 사용할 수 있고 오작동이 보고되었는지 확인 (신뢰성) -저장된 개인 정보는 시스템 오작동으로 인해 손상 될 수 없음을 보증 (데이터 무결성) -주문에서 처리 된 개인 데이터는 고객의 지시에 따라 처리 될 수 있음을 보장 (주문 관리) -개인 데이터가 파손 또는 손실로부터 보호되는지 (가용성 제어) -다른 목적으로 수집 된 개인 데이터가 개별적으로 처리 될 수 있는지 확인 (분리 가능)	BDSG 제9조 부속서
손해배상	GDPR과는 달리, 근로자에 대한 청구가 새로 포함되며, 피해자는 금전적 손해가 아닌 손해로 인해 적절한 보상을 요구할 수 있음. (자동 처리가 아닌 경우 책임자의 과실로 인한 손해를 배상 할 수 없는 경우 배상 책임을 면제됨)	BDSG 제83조 제2항

예를 들어, GDPR에서 아동은 “특별한 보호”를 받을 자격이 있는 “취약한 개인”으로 간주되기 때문에, 아동 데이터를 처리하는 것은 민감한 주제에 해당

된다. 하여, GDPR은 온라인 서비스를 제공하는 컨트롤러 등에게 16세 미만의 아동 동의를 받을 때에는 그 아동에 대한 책임이 있는 부모 등의 동의를 얻도록 요구하고 있다(제8조(2)). 그러나 이 조항도 회원국에게 재량을 허용하는 위임을 하고 있는데, 이 경우에도 13세 미만까지가 회원국에게 허용된 재량의 범위가 된다.

Ⅳ. EU의 GDPR과 현행법의 발전방향

1. 정보주체의 권리보장

현행 「개인정보보호법」제5장과 <표3>에서 기술한 EU의 GDPR의 정보주체 권리보장을 비교하면, EU의 GDPR이 기본권인 개인정보자기결정권과 알권리를 두텁게 보호하는 방안을 마련하고 있는 것으로 보인다. 즉, EU의 GDPR은 제3장을 통해, 개인정보의 이동권(right to data portability)[33], 처리제한에 대한 권리, 반대권(반대할 권리;right to object), 프로파일링을 포함한 자동화된 의사결정 관련 권리(automated individual decision-making, including profiling) 등의 정보주체 권리를 보장하고 있는데, 이는 우리나라의 현행법제 보다 폭넓게 정보주체의 권리를 보장하고 있는 것으로 요약분석하면 다음과 같다. 첫째, GDPR의 제20조에 규정된 개인정보의 이동권(데이터 이동권)을 현행 「개인정보보호법」상의 제3자 제공 조항은 제17조, 목적외 이용ㆍ제공 조항인 제18조, 국외 이전에 관한 조항인 제19조와 연관시켜 생각해 볼 수 있으나, GDPR이 빅데이터의 활성화와 맞물려, 온라인 서비스에 대한 정보주체의 선택권을 확대하기 위해 신설된 조항이라는 점에서, 현행 「개인정보보호법」상의 제17조~제19조의 조항이 해당 "개인정보처리자"가 정보주체의 동의 등(및 그 외 법령 등이 허용하는 사유)에 의해 개인정보를 처리하는 것에 주안점을 두고 있다면, GDPR의 제20조의 개인정보의 이동권(right to data portability)은 처리가 자동화된 수단에 의해 수행되는 것을 전제로 정보주체에게 선택권이 있어, 정보주체가 주도적으로 자신의 정보를 제3자에게 제공해 줄 것을 요청할 수 있다는 점에서 차이가 있다. 둘째, GDPR 제21조에서 규정하고 있는 반대권(right to object)의

33) "Right to data portability"는 개인정보의 이식권으로 해석되기도 하였으며, 최근 개인정보의 이동권으로 번역되어 쓰이고 있으나, '개인정보의 이전권'으로도 해석이 가능함.

경우 정보주체가 자신의 “특수한 상황”에 근거하여 개인정보의 처리에 반대할 수 있는 권리로, 현행 「개인정보보호법」상의 제36조(개인정보의 정정·삭제)·제37조(개인정보의 처리정지)와 유사하지만, 그 처리(프로파일링 포함)가 직접 마케팅을 목적으로 한 것 외에 일반적으로 그 처리가 공익목적이라 하여 허용되고 있는 ‘과학 또는 역사연구·통계 목적의 개인정보 처리에 있어서도, 해당 처리가 공익목적을 위해 반드시 필요한 경우가 아니라면, 정보주체가 본인의 특수한 상황에 근거해 언제든지 반대권을 행사할 수 있도록 하고 있다는 점에서 우리나라의 현행 정보주체의 권리보장 법제와 차이가 있으며, 개인정보처리자에게 그 처리에 관한 입증책임을 부과하고 있다는 점에서 정보주체의 권리를 두텁게 보호하고 있다. 셋째, GDPR 제22조의 ’프로파일링을 포함한 자동화된 의사결정 관련 권리(automated individual decision-making, including profiling)‘는 프로파일링을 포함한 자동화된 개인정보의 처리가 정보주체 자신에게 법적 효력 또는 이와 유사한 효력을 초래하여 자신에게 중대한 영향을 끼치게 되는 경우, 그러한 의사결정의 적용을 배제할 수 있는 권리로, 제4차 산업혁명시대에 빅데이터와 AI 등을 통한 자동화된 처리방식으로부터 정보주체의 자유와 권리를 두텁게 보호하고 있다는 점이 특징으로 현행 「개인정보보호법」상으로는 제35조의 열람을 통해, 제36조와 제37조를 적용해 정정·삭제, 처리정지할 수 있는 정도 밖에 없다는 점에서, GDPR 제22조의 ’프로파일링을 포함한 자동화된 의사결정 관련 권리(automated individual decision-making, including profiling)‘는 우리나라의 법제에도 도입이 필요한 권리보장 방안이라 할 수 있다. 마지막으로 GDPR의 제18조 처리제한권(right to restriction of processing)의 경우, 정보주체가 자신의 정보에 대해 개인정보처리자에게 해당 정보의 정확성에 대해 이의제기하거나, 처리가 불법적이지만 해당 개인정보에 삭제를 원하는 대신 이용제한을 요청한 경우, 개인정보처리자가 그 처리목적을 달성했음에도 그 청구권의 입증·방어 등을 위해 요구하는 경우 등에 있어서는 처리의 제한을 할 수 있도록 하는 권리로, 현행법 「개인정보보호법」상으로는 제35조의 열람을 통해,정정·삭제, 처리 정지할 수 있는 정도(법 제36조·제37조)밖에 없다는 점에서, 이 또한 우리나라 개인정보보호법제에 도입이 필요한 정책이라 할 수 있다.

지금까지 살펴본 바에 따라 GDPR 상의 정보주체 권리 보장제도 중 우리나라에도 적용이 필요한 권리보장방안을 살펴보면, 첫째, 개인정보의 이동권(데이터 이동권, right to data portability)의 경우 IoE시대에 부합되는 개념으로, 정보주체 자신의 목적을 위해 개인데이터의 재사용을 요구할 수 있도록 권리

를 부여하는 것이나(현행법상 「개인정보보호법」제18조에 따른 목적 외 이용 및 제공이 여기에 해당되나, 이는 개인정보처리자가 별도의 동의를 얻어야 한다는 점에서, 정보주체의 요구권을 부여하는 GDPR상의 개념과 차이가 있음), 둘째, 일명 잊힐 권리라 불리는 '삭제권'도 '아동에 대한 정보 제공 서비스' 등에 대한 적용영역의 확장을 고려해 볼 필요가 있다. 셋째, GDPR상의 '반대할 권리(right to object)'의 경우, 개인이 자신의 개인데이터의 처리와 관련해, '자신의 특정 상황'에 근거해, 이미 처리되고 있는 개인데이터에 이의를 제기할 수 있도록 한다는 점에서, IoE시대에 효과적으로 대응하기 위해 '포괄적 동의'를 도입하자는 여타의 견해에 '정보주체의 권리보호' 역할을 수행하는 제어장치로 작용할 수 있을 것이라 판단된다. 그 외에도 현재의 법제와 유사점이 있으나, 그 보호의 범위나 방법에 차이가 있는 부분은 우리나라의 환경을 고려하여, 도입여부를 따져볼 필요가 있다. 결과적으로 GDPR에서는 보장하지만, 현재 우리나라에는 없는 정보주체의 권리보장제도는 4차 산업혁명을 주도하고자 현 정부가 준비하고 있는 공공기관의 데이터처리와 관련되어 도입을 고려해볼 필요가 있다.

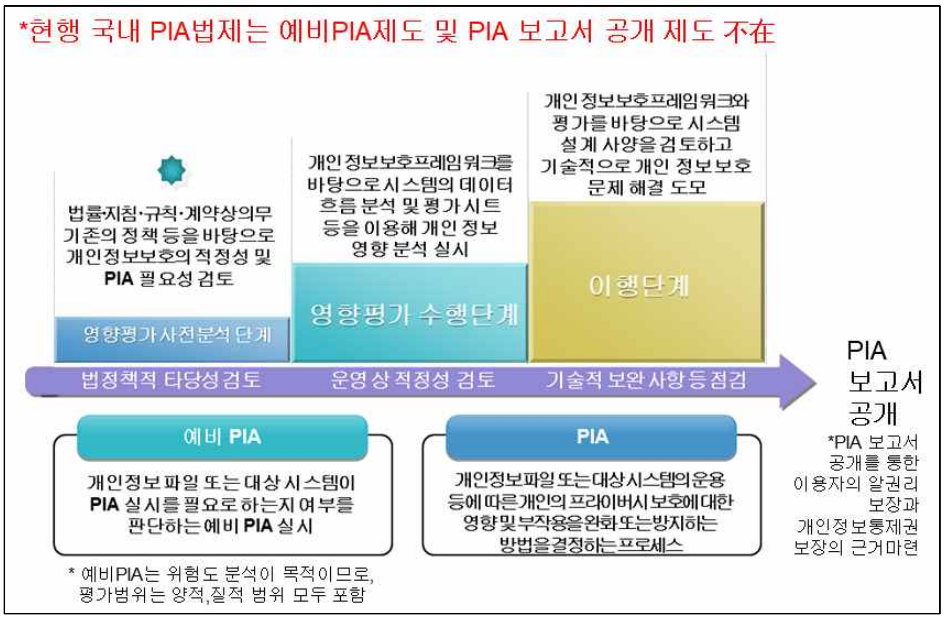
2. 개인정보영향평가(PIA) 제도

개인정보영향평가(PIA)는 현행 「개인정보보호법」에 따를 때, "개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인을 분석하고 개선사항을 도출하기 위한 평가"(법 제33조제1항)하는 것이다. 이는 "개인정보 수집ㆍ활용이 수반되는 사업 추진 시 개인정보 오남용으로 인한 프라이버시 침해 위험이 잠재되어 있지 않는지를 조사ㆍ예측ㆍ검토하고 개선하는 제도"(개인정보보호법 해설서[34])이다. 그러나 구「공공기관의 개인정보에 관한 법률」이 시행되다, 2011년 일반법인 「개인정보보호법」이 제정되어 시행되며, PIA를 도입하다보니, 기존에 만들어진 개인정보파일/시스템에 대해 그 적용이 이뤄지게 되어(공공기관의 경우 일정한 요건에 해당될 경우, 의무적으로 2016년 9월 30일까지 법정 평가기관에 의한 PIA를 받도록 하였음), 사후 추인하는 형식의 영향평가가 그동안 실시되었다. 이는 PIA의 근본취지를 무색하게 하는 것으로, PIA는 일반적으로 <그림1>의 구조를 띄고 운영되고 있으며, <표7>에서 확인할 수 있는 바와 같이, 그 적용대상과 범위가 우리나라의

34) 행정자치부, 개인정보보호법 해설서, 2016, 268면.

현행 PIA제도에 비해 GDPR과 'PIA 국제표준(International Standard ISO/IEC 29134)'이 확대되어 실시되고 있다.

<그림1> PIA의 프레임워크와 현행법제의 문제점



우리나라와 EU의 GDPR 그리고 'PIA 국제표준(International Standard ISO/IEC 29134)'을 비교하면, <표7> 과 같다.

<표7> 국내제도와 PIA국제표준/DPIA비교

구분	국내제도	PIA국제표준	GDPR
대상	의무: 공공기관 권고: 민간 개인정보처리자	공공기관과 민간 등 개인정보처리자	공공기관과 민간 등 개인정보 컨트롤러,프로세서
대상	1. 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일 : 구축·운용 또는 변경하려는 개인정보파일에 5만명 이상의 정보주체에 관한 개인정보가 포함된 경우 2. 다른 개인정보파일과 연계하려는 경우: 해당 공	아래의 사항과 관련 고려사항을 검토하여 PIA실시 여부 결정 - 개인정보를 처리하거나 처리될 예정인 신규 또는 새로운 기술, 서비스 또는 기타 사업 - 민감한 개인정보 처리된다는 결정	GDPR의 경우 데이터 처리 대상에 대한 높은 위험도를 초래하는 새로운 처리 활동이 제안 된 경우(특히 신기술이 사용될 경우, WP 248 "영향 평가 지침 "에 따를 때),아래의 요건에 해당할 때, 영향평가를 실시토록 의무화 하고 있음.

	공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계한 결과 50만명 이상의 정보주체에 관한 개인정보가 포함된 경우 3. 일반적인 개인정보 파일: 구축·운용 또는 변경하려는 개인정보파일에 100만명 이상의 정보주체에 관한 개인정보가 포함된 경우 4. 영향평가를 받은 후 개인정보 검색 체계 등 개인정보파일의 운용 체계를 변경하려는 경우: 해당 개인정보파일 중 변경된 부분	- 적용되는 개인정보보호관련 법규의 변경, 회사정책 및 표준정보시스템의 운용 데이터 처리 목적 및 수단, 신규 또는 변경된 데이터 흐름 등 - 사업 확대 또는 인수	- 정보주체의 평가 (예: 직장에서의 수행, 건강, 행동 또는 위치) - 자동화된 의사 결정 (예 : 자동거부) - 체계적인 모니터링 (특히 은밀한 모니터링)/민감한 개인 데이터 처리/대규모 처리/별도의 데이터 세트를 결합하거나 매칭하는 것/취약한 개인에게 영향을 미치는 처리/시험되지 않은 기술을 사용하여 처리/국경 간 데이터 전송
PIA 보고서 공개	공개는 의무가 아님	공개토록 함	공개토록 함

PIA가 개인정보의 처리나 시스템의 설계 시에 위험도를 분석하여, 개인정보 오남용으로 인한 프라이버시 침해의 잠재적 위험을 사전에 분석·예측·대응하도록 한다는 점에서, 현행법을 개정하여, 영향평가 대상을 확대하고, 공공기관별 PIA의 실시여부를 결정하는 사전검토방안을 강구할 필요성이 있으며, 민간 개인정보처리자의 영향평가 의무화 방안 마련 (안전성 확보조치 고시 상의 유형별 대응)하고, GDPR의 경우 영향평가의 결과는 공개해야 하고, 감독기구와 사전협의한 경우 해당 감독기구에 이를 제공해야 한다는 점[35]에서 PIA보고서의 공개를 통해 정보주체의 알권리를 보장할 필요가 있다. 더불어 EU의 GDPR과 같이 일정한 요건에 해당할 경우(<표7> 참조), PIA를 의무화하고 이에 대한 결과를 공표하는 방안을 마련할 필요성이 있다. 더불어 행안부/인터넷진흥원 주도로, EU집행부와의 협의를 통해, 본 국제표준에 맞는 우리나라의 영향평가 표준을 만들고, 이 절차를 밟아 PIA를 실시한 경우, GDPR에서 요구하는 DPIA를 수행한 것으로 간주하는 절차를 마련할 필요성이 있다. 이는 유럽 등을 진출하는 국내 기업에 부담을 경감시켜주는 효과가 있으며, 제4차 산업혁명 시대를 대비하며, 기술발전과 개인의 권리보장이라는 가치에 황금률을 정하는 척도로 작용할 것이라 생각한다.

35) 영미법계 국가인, 미국·캐나다 등도 영향평가의 결과는 공개토록 하고 있음.

Ⅴ. 결론

현재 우리나라는 제4차 산업혁명을 준비하며, 정보통신의 기술발전에 주안점을 두고 모든 정책을 준비 중에 있다. 이는 급변하는 세계정세에 대비하고, 정치·경제·문화적 측면 등 전방위적인 국가발전과 국민 개개인의 복지환경 구현을 위해 불가피한 선택이라 할 수 있다. 그러나 정보통신 발전(순기능)에 드리우게 될 그림자(역기능)를 살펴, 가능한 발전과 맞바꿀 수 없는 가치(인간의 존엄과 가치 및 이에 근거한 개개인의 프라이버시권 보장)가 훼손되지 않도록 하는 거버넌스적 차원의 대책마련이 필요하다.

이러한 상황을 고려할 때, EU의 GDPR은 정보통신발전을 수용하면서도, 정보주체의 인권보장을 폭넓게 고려하고 있다는 점에서, 현재의 법제에 필요한 범위 내의 수용을 고려해 볼 필요가 있다. 즉, 정보주체의 기본권 보장을 위한 '개인정보의 이동권(right to data portability), 처리제한에 대한 권리, 반대할 권리, 자동화된 결정 및 프로파일링관련 권리' 등의 우리나라 법제에 맞는 도입과, PIA의 적용대상과 범위 및 적용 방식의 개선안 마련이 그것이다.

무엇보다 PIA의 경우 정보주체의 알권리보장과 개인정보자기결정권의 보장을 위해, (ⅰ) 평가 대상을 확대하고, (ⅱ) 공공기관별 PIA의 실시여부를 결정하는 사전검토방안을 강구할 필요성이 있으며, (ⅲ) 민간 개인정보처리자의 영향평가 의무화 방안 마련(안전성 확보조치 고시 상의 유형별 대응)하고, (ⅳ) GDPR의 경우 영향평가의 결과는 공개해야 하고, (ⅴ) 감독기구와 사전협의한 경우 해당 감독기구에 이를 제공해야 한다는 점에서 PIA보고서의 공개를 통해 정보주체의 알권리를 보장할 필요가 있다(이 때에 EU의 GDPR상의 opening 조항들과 우리나라 개인정보보호법제를 비교하여, 그 간극을 보충할 필요성 있음). 더불어 행안부/인터넷진흥원 주도로, EU집행부와의 협의를 통해, 본 PIA 국제표준에 맞는 우리나라의 영향평가 표준을 만들고, 이 절차를 밟아 PIA를 실시한 경우, GDPR에서 요구하는 DPIA를 수행한 것으로 간주하는 절차를 마련할 필요성이 있다.

시대가 변하고 그 변하는 시대에 대처하기 위한 국민을 포함한 국가구성원의 노력은 동서고금을 막론하고 계속되었다. 현재 우리나라가 제4차 산업혁명 시대를 논하고 이에 대비하고 있지만, 역사적 관점에서 살펴보면, 발전에만 방점을 두고 대안을 마련할 경우 돌이킬 수 없는 가치의 훼손을 대체할 그 무엇인가는 존재하지 않는다는 점에서, 국민 개개인의 사생활의 자유 등 프라이버

시 보호를 통한 인간의 존엄과 가치를 보장하는 정책을 고려하는 것이 조금은 늦더라도 가장 빠른 길일 수 있음을, 방향을 잘못 잡고 발전에만 힘을 쏟아 돌이킬 수 없는 상황에 직면한 때에야 비로소 깨닫지 않기를 바란다.

[참고문헌]

권건보, “개인정보자기결정권”, 헌법재판연구원, 기타발간자료, 107~143, 2012.

김유민/이기동, “디지털 정보시대에서 잊혀질 권리의 인식 비교 평가”, 국제e-비즈니스학회, e-비즈니스연구 15(4), 2014.

손형섭, “개인정보의 보호와 그 이용에 관한 법적 연구”, 한국법학회, 법학연구 54, 2014.

정영화, “헌법상 정보 프라이버시로서 ‘잊혀질 권리’”, 경북대학교 법학연구원, 법학논고 39, 2012.

조수영, “개인정보보호법에서의 정보주체의 동의와 기본권 보장에 관한 연구”, 한국법학회, 법학연구 제18권 제1호(통권 69호), 2018.

차상육, “빅데이터(Big Data) 환경과 프라이버시의 보호”, 「IT와 법연구」 제8집, 경북대학교, 2014.

최혜민, “빅데이터 시대와 현행 개인정보보호법제의 부정합 문제 및 그 해결방안에 대한연구”, 「IT와 法연구」 제8집, 경북대학교, 2014.

행정자치부/한국인터넷진흥원, 『우리 기업을 위한 유럽 일반개인정보보호법(GDPR)』 안내서, 2017,

행정자치부, 개인정보보호법 해설서, 2016.

Christopher Kuner, “Data Protection Law and International Jurisdiction on the Internet (part1)”, International Journal of Law and Information Technology, Oxford University Press, Vol. 18. No.2, pp. 176~193

Daniel J. Solove., 『Understanding privacy』, Harvard University Press, 2008.

Erwin Chemerinsky, 『Constitutional Law: Principles and Policies』, Aspen Law & Business, 2002.

———, “Data Protection Law and International Jurisdiction on the Internet (part2)”, International Journal of Law and Information Technology, Oxford University Press, Vol. 18. No.3, pp. 227 ~ 247

Michael Griffin, “Digital Eraser? European Court Endorses the 'Right to be Forgotten'”, JETLaw: Vanderbilt Journal of Entertainment & Technology Law, June 10, 2014.

Michael Butterworth, “The ICO and artificial intelligence: The role of fairness in the GDPR framework”, Computer Law & Security Review Volume

34, Issue 2, 2018, pp. 257-268,

Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, Ignacio Sanchez, “The right to data portability in the GDPR: Towards user-centric interoperability of digital services", Computer Law & Security Review, Volume 34, Issue 2, April 2018, pp. 189-432.

Richard Warner/Robert H. Sloan, “Beyond Notice and Choice: Privacy, Norms, and Consent", 14 Journal of High Technology Law 370, 2014.

Robert H. Sloan/Richard Warner, Big Data and the “New” Privacy Tradeoff, Chicago-Kent College of Law Research Paper No. 2013-33, August 5, 2013.

wp248(ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679).

William L. Prosser, Privacy, 48 Cal. L. Rev. 383 - 423(1960).

牧田潤一郎, “アメリカのプライバシー保護法制の日本への示唆”, 「Law and Practice」 第4号, 2010.

ISO/IEC, International Standard ISO/IEC 29134, 2017.

石井夏生利,『個人情報保護法の現在と未來 世界的潮流と日本の將來像』, 勁草書房, 2014年 7月.

_____, 「ビッグデータと個人情報保護」 予防時報第258号 2014年 夏号「パーーーー, ソナルデータの利活用における技術および各國法制度の動向:2.アメリカのプライバシー保護に關する動向」情報處理第55卷12号 2014年11月.

芦部信喜, 『憲法 第三版』 , 岩波書店, 2002.

https://www.dbpia.co.kr

https://www.priv.gc.ca

http://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1

https://www.legifrance.gouv.fr/

http://www.servat.unibe.ch/dfr/bv065001.html

http://www.jetlaw.org/2014/06/10/digital-eraser-european-court-endorses-the-right-to-be-forgotten/

https://ico.org.uk/
https://dsgvo-gesetz.de/bdsg-neu/
https://eugdprcompliant.com/

[Abstract]

A Study on Privacy Protection in the EU's GDPR and Korea's Personal Information Protection Act

Cho, Soo-Young*

The era of the 4th Industrial Revolution is an epoch when information becomes a resource and power by the advancement of information and communication technology. And personal information(data) is an important axis for this information flow. And personal information(data) is an important axis for this information flow.

However, if the personal information is used only well, it is a means of providing the best service for the pursuit of happiness of the data subject, but if it is abused, it can lead to serious privacy invasion and disturb human dignity and worthiness. So personal information(data) is like a double-edged sword. It is necessary to make a policy effort to maximize the pure function and to minimize the dysfunction. Meanwhile, the EU has enacted a statutory GDPR for the efficient operation of the personal and information functions, and all member countries will implement it from May 25, 2018.

In this paper, I study on the EU's GDPR(including data protection impact assessments; DPIAs) and compare with Korea's Personal Information Protection Act for the protection of the self-determination right and the right of knowing which are basic rights of the people effectively in response to the 4th Industrial Revolution era.

Keywords : Personal information protection, General Data Protection Regulation(GDPR), Personal information right of self-determination, right to know, personally identified information, personally identifiable information, right to be forgotten, Right to restrict processing, Right to data portability, privacy impact

* Dr. Jur. A non-term professor in Sookmyung Women's University

assessment(PIA), Data protection impact assessments (DPIAs), International Standard ISO/IEC 29134