「 '4차 산업혁명'과 정보인권 」 연속토론회

빅데이터 시대 이용자의 권리
- 프로파일링 규제를 중심으로

일 시 | 2017년 8월 17일(목) 오전 10시~12시

장 소 | 국회의원회관 제1세미나실

주 최 |

국회 과학기술정보방송통신위원회
변재일 의원 (더불어민주당, 충북 청주시청원구)
김성수 의원 (더불어민주당, 비례대표)
추혜선 의원 (정의당, 비례대표)
국회 행정안전위원회
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

10:00 ~ 10:05	개회	
10:05 ~ 10:15	인사말	
	사회	김기중	국가인권위원회 비상임위원
10:15 ~ 10:45	발제	박노형	고려대학교 법학전문대학원 교수
10:45 ~ 11:45	토론	김보라미	언론연대 정책위원, 변호사
		전응준	법무법인 유미 변호사
		차상육	경북대학교 법학전문대학원 교수
		심우민	국회 입법조사처 입법조사관
		이원태	정보통신정책연구원 ICT전략연구실 연구위원
11:45 ~ 12:00	전체토론	

김성수 | 더불어민주당 국회의원

안녕하십니까.

국회 과학기술정보방송통신위원회 소속 더불어민주당 국회의원 김성수입니다.

‘4차 산업혁명’과 ‘개인정보 보호 강화’를 조화와 미래 신기술로부터 국민의 정보인권을 보호할 수 있는 방안 모색을 위해 기획된 「‘4차 산업혁명’과 정

보인권」 연속토론회가 벌써 4회차를 맞이하고 있습니다. 꾸준한 관심을 보내주신 각계각층의 관계자 여러분께 깊은 감사 인사를 드립니다.

오늘 토론회는 프로파일링 거부권 등 미래신기술에 대비한 개인정보보호법의 개선 방향을 논의하는 자리입니다. 빅데이터 시대에 다양한 가치를 창출하는 개인정보의 활용은 필연적 요소입니다. 향후 빅데이터 산업 활성화에 대한 모든 논의과정에서 '사회적 합의절차'가 필요할 것이라고 생각합니다. 일방적인 규제 강화나 완화가 아니라 정보주체인 국민 개개인의 '개인정보자기결정권'을 합리적으로 보호하여 빅데이터 활용에 대한 균형을 찾는 것이 중요합니다.

특히 내년 5월 28일에는 EU 28개 전 회원국에 공통적으로 적용되는 유럽 일반개인정보보호규칙(GDPR)의 시행이 예정되어 있습니다. 한국을 비롯한 글로벌 기업들은 EU 역내·외에서 경제활동을 하는 경우 강화된 GDPR을 준수해야 하기 때문에 개인정보를 처리하는 기업은 프로파일링(profiling) 규정 등에 큰 영향을 받을 것으로 예상됩니다.

그러나 한국은 아직 준비 정도가 미흡하다는 평가를 받고 있습니다. GDPR 시행까지 1년도 채 남지 않았지만 법 개정을 비롯해 정부 부처 내 합의, 기업들의 인식제고 등 갈 길이 멀다는 우려가 나오고 있습니다.

이번 토론회를 통해 GDPR에 대한 올바른 이해가 이뤄질 수 있기를 기대합니다. 또한 프로파일링 제도를 중심으로 한 해외입법례 비교를 통해 미래

신기술에 대비한 개인정보보호법 개선에 대한 방향이 마련될 수 있기를 바랍니다. 저 역시 우리의 법제가 EU와 같이 데이터의 올바른 활용은 보장함과 동시에 국민의 개인정보는 안전하게 보호될 수 있도록 국회에서 힘을 보태도록 하겠습니다.

끝으로 오늘 토론회를 공동 주최해주신 더불어민주당 변재일, 진선미, 이재정 의원, 국민의당 권은희 의원, 정의당 추혜선 의원과 언론개혁시민연대, 정보인권연구소, 진보네트워크센터, 참여연대, 한국소비자단체협의회, 함께하는 시민행동 등 시민사회단체 관계자 여러분께 감사드립니다. 또한 발제를 맡아주신 고려대학교 법학전문대학원 박노형 교수님과 토론자 여러분께 다시 한 번 감사의 말씀을 드립니다.

이효성 | 방송통신위원회 위원장

안녕하십니까,

방송통신위원회 위원장 이효성입니다.

먼저 ‘빅데이터 시대 이용자의 권리’라는 주제로 열리는 오늘 토론회 개최를 진심으로 축하드리며, 소중한 자리를 마련해주신 김성수 의원님과 관계자 여러분들께 깊은 감사의 말씀을 드립니다.

오늘 토론회는 ‘4차 산업혁명과 정보인권’이라는 큰 주제 아래 네 번째로

치러지는 연속토론회입니다.

‘4차 산업혁명’은 우리 사회와 경제에서 중요한 담론 가운데 하나로 자리 잡고 있습니다. 초연결성과 지능화를 특징으로 하는 4차 산업혁명 시대에는 데이터가 미래 경쟁력의 핵심이 됩니다. 국가 경쟁력을 제고하고 사물인터넷, 빅데이터 등 4차 산업혁명 관련 산업을 성공적으로 이끌기 위해서는 개인정보를 비롯한 데이터의 다양한 활용이 필수적인 점은 부인하기 어렵습니다.

한편 개인정보 활용 서비스가 점점 더 복잡해지고 기술이 고도화되는 사회에서 한 명, 한 명의 이용자들은 개인정보 및 프라이버시 침해에 대한 불안감을 더 크게 느낍니다. 특히 개인의 경제적 상황, 관심, 행동 등을 분석하거나 예측하기 위하여 정보를 이용하는 프로파일링은 특정인에 대한 낙인 또는 차별, 감시, 정보선택권 제한 등 새로운 프라이버시 위험 요소가 될 수 있습니다.

최근 유럽에서 제정하여 내년 시행을 앞두고 있는 일반개인정보보호규정(General Data Protection Regulation, 이하 GDPR)’은 개인정보 분야의 유익한 참고서가 될 수 있습니다.

GDPR은 프로파일링을 명시적으로 정의하면서 정보주체를 보호하기 위한 장치들을 마련하고 있습니다. 뿐만 아니라 프라이버시 중심 설계(Privacy by Design)를 도입하여 ICT 환경에서의 개인정보 보호에 대비하고 있습니다.

4년간의 논의 끝에 GDPR은 시장 환경 변화를 반영하여 EU 회원국간 개인정보의 자유로운 이동을 보장하는 동시에 정보주체의 개인정보 보호 권리를 강화하는 내용으로 마련될 수 있었습니다.

우리나라도 데이터 기반 4차 산업혁명에 장애가 되지 않으면서도, 정보주체의 권익을 실질적으로 보장하기 위한 정책을 강구해야 합니다.

방송통신위원회에서는 신규 ICT 기술발전에 따라 새로이 대두되는 개인정보보호 이슈에 선제적으로 대응하기 위하여 「온라인 맞춤형 광고 개인정보보호 가이드라인('17.2월)」, 「스마트폰 앱 접근권한 개인정보보호 안내서('17.3월)」 등을 마련하였고, 지문·홍채 등 생체인식정보를 보호하기 위한 가이드라인도 준비하고 있습니다.

기술의 빠른 발전으로 개인정보 관련 신규 이슈가 늘어남에 따라, 개인정보 침해 위협을 실질적으로 해소할 수 있는 정책이 필요하다는 사회적 목소리가 점점 더 커지고 있음을 경청하고, 개인정보를 실질적으로 보호하면서도 안전하게 활용할 수 있는 규제체계를 마련하기 위해서 만전을 기하도록 하겠습니다.

오늘의 토론회를 통해 빅데이터 시대의 개인정보 보호를 위한 다양한 의견들이 모여 우리나라가 IT, 인터넷에 이어 개인정보 분야에서도 진일보할 수 있는 소중한 계기가 마련되기를 기대하며, 방송통신위원회도 오늘 토론회

에서 이루어지는 논의를 정책에 반영할 수 있도록 노력하겠습니다.

다시 한번 토론회 개최를 축하드리며, 토론회에 참석하신 모든 분들께 건강과 행운이 함께하기를 기원합니다. 감사합니다.

빅데이터 분석기술의 관점에서 EU GDPR의 프로파일링에 관한 규정 검토 (초고)[1)]

박노형 | 고려대학교 법학전문대학원 교수

1. GDPR 일반

개인정보보호에 관하여 유럽연합 (European Union: EU)이 가장 적극적이고 체계적인 법제도를 가지고 있음에 별다른 이의가 없을 것이다. EU회원국들은 1995년 'EU지침 95/46' (이하 '1995년 지침')을 국내입법을 통하여 시행하고 있는데, EU 내에서의 개인정보보호 수준을 높이면서 관련 법제도의 통일적 적용을 위하여 유럽위원회는 2012년 1월 'EU 개인정보보호 개선' (EU Data Protection Reform)을 제시하였다. 이후 유럽위원회, 유럽의회 및 EU이사회 사이의 긴밀하고 집중적인 협상을 통하여 채택된 'EU규칙

1) 본 발제문은 아직 완성되지 않고 발전 중에 있습니다.

2016/679’ (General Data Protection Regulation, 일반개인정보보호규칙: 이하 ‘GDPR’)은 2016년 5월 24일 발효하였고 2018년 5월 25일부터 적용된다.

GDPR은 1995년 지침의 채택 이후 특히 인터넷의 보편적 사용 등에 따른 개인정보 처리의 환경 변화를 반영하여 정보주체를 보호하면서 동시에 개인정보를 처리하는 사업자 등 컨트롤러 (controller)의 개인정보 이용을 촉진함으로써 민주사회의 개인정보보호에 있어서 개인과 사회의 이익을 균형되게 보호하려고 한다.[2] 개인정보보호의 방향 등을 두고 미국과 치열한 경쟁을 하고 있는 EU의 GDPR은 개인정보보호의 새로운 지평을 열어서 한국 등 국제사회에 큰 영향을 줄 것이다. 특히 상품과 서비스에 이어서 데이터 무역에 대한 국제규범이 생성되는 과정에서 더욱 활성화될 개인정보의 국경간 이전은 새로운 국제경쟁력의 기준이 될 것이어서 GDPR의 올바른 이해는 더욱 절실하다.

아래 프로파일링에 관한 구체적인 내용의 검토에 앞서서 GDPR의 개인정보보호에 대한 원칙의 이해가 필요하다. 첫째, 개인정보의 처리에 관련하여 자연인의 보호는 기본권이고, 모든 사람은 자신에 관한 개인정보의 보호에 대한 권리를 가진다.[3] GDPR은 ‘자유, 안전 및 정의 지역’ (an area of

---

2) EU에서 컨트롤러는 개인정보보호법의 개인정보처리자로 이해할 수 있다.

3) GDPR 상설 제1항. 특히 EU기본권헌장 (Charter of Fundamental Rights of the European Union) 제8(1)조와 EU기능조약 (Treaty on the Functioning of the European Unioin) 제16(1)조 참조. 흥미롭게도, 1995년 지침은 정보주체를 남성으로서 표시하는데, GDPR은 남성과 여성 모두로 표시한다.

freedom, security and justice)과 '경제연합' (an economic union)의 완성, 경제사회적 진전, 내부시장 내의 경제체제의 강화와 통합, 및 자연인의 복지에 기여하고자 한다.[4] 따라서 EU에서 개인정보보호는 그 자체를 위하여만 존재하는 것이 아니고 경제사회적 통합에 기여하여야 한다. 개인정보의 수집과 공유의 규모가 상당하게 증가하는 등 급속한 기술적 발전과 세계화는 개인정보 보호에 대한 새로운 도전이 되었는데,[5] 그 결과 디지털경제가 내부시장에 걸쳐 발전할 수 있게 하는 신뢰가 창출되는 중요성을 고려하여 강력한 집행이 지지하는 'EU 내의 강력하고 보다 일관된 개인정보보호프레임워크' (a strong and more coherent data protection framework in the Union)가 요구된다.[6] 자연인은 자신의 개인정보를 통제하여야 하고, 자연인, 경제주체 및 공공당국을 위한 법적 및 실제적 안정성이 제고되어야 한다.[7] 이렇게 GDPR은 본연의 목적은 자연인의 개인정보보호이지만, 개인정보를 처리하는 경제주체와 공공당국 등 컨트롤러의 법적 안정성도 함께 고려하여, EU의 궁극적인 목적인 회원국들 사이의 완전한 통합에 기여하고자 한다.

2018년 5월 25일 GDPR이 적용되면, 빅데이터 산업은 사실상 죽음이라는 다소 무서운 주장이 제기되고 있는데, 빅데이터 산업의 대표적 기업들, 예컨대 주요 IT기업들이 미국에 기반을 둔 점에서 GDPR의 적용으로 미국 기업들이 큰 타격을 입을 것이라고 한다. 그런데, 이러한 주장은 일견 이해될 수

4) GDPR 상설 제2항.

5) GDPR 상설 제6항.

6) GDPR 상설 제7항.

7) GDPR 상설 제7항.

있지만, 그렇다고 정당하다고 수용될 수 없을 것이다. 물론 GDPR이 정보주체의 동의와 프로파일링을 포함한 자동화된 처리에만 기초한 결정에 관한 규정 등에서 정보주체의 개인정보자기결정권을 강화한 만큼 개인정보를 이용하는 기업 등 컨트롤러에게 장애가 되는 것은 맞지만, 아래에서 검토되듯이 이러한 장애는 컨트롤러에게 극복할 수 없도록 엄격하다고만 볼 수 없다. 개인정보의 이용으로 이익을 얻는 컨트롤러는 이에 대한 대가로서 개인정보보호에 대한 투자를 함으로써 이러한 장애를 극복해야 할 것이기 때문이다. 개인정보보호에 있어서 자연인인 정보주체의 권리 강화를 IT기업 등 컨트롤러의 사업 추구에 대한 제한이라고 비난하는 것은 개인정보를 포함한 정보가 핵심인 21세기 디지털경제에서 수용할 수 없을 것이다.

GDPR은 EU의 법으로서 제1차적으로 주로 EU 기업들인 컨트롤러에게 적용되지만, 역외적용의 확대로 미국 기업은 물론 한국 기업에게도 적용될 수 있다. 따라서 미국 기업에게 불리하게 적용된다는 GDPR은 EU 기업에게도 불리하게 적용되는 것이다. 그러나, GDPR이 자신의 제1차적 수범자인 EU 기업에게 불리하도록 제정되어 적용된다는 것은 기대하기 어렵다. GDPR은 그 적용 대상이 개인정보 처리에 관한 자연인의 보호 및 개인정보의 자유로운 이동이고 개인정보보호가 인간의 기본권이며, 1995년 지침과 마찬가지로, 특히 EU 역내에서의 개인정보의 자유로운 이동이 개인정보 처리에 관한 자연인의 보호에 연계되는 이유로 제한하거나 금지되어서는 안된다고 규정한다.[8] 또한, EU는 GDPR의 채택과 함께 소위 '단일디지털시장' (single

8) GDPR 제1조 및 1995년 지침 제1(2)조 참조. 이와 달리 개인정보보호법은 개인의 자유와 권리

digital market)의 완성을 위하여 많은 노력을 경주하고 있다.[9] 이런 점에서 예컨대 유럽위원회의 2012년 GDPR 초안에서 모든 개인정보 처리에 정보주체의 명시적 동의를 요구하도록 제안되었으나, 회원국들 이익을 대표하는 EU이사회와의 최종담판에서 결국 민감정보의 처리 등 특별한 경우에 정보주체의 명시적 동의를 요구하도록 타협을 이루었다. 따라서, GDPR은 그 자체로 정보주체의 자신의 개인정보에 대한 통제를 강화하면서 동시에 그 개인정보를 이용하는 기업 등 컨트롤러의 정당한 이익이 부당하게 침해되지 않도록 나름의 균형을 이루었다고 보아야 한다. 이러한 균형은 GDPR의 프로파일링에 관한 규정에서도 확인된다.

또한, 개인정보 보호에 대한 권리는 절대적이 아니어서, 비례성 원칙에 따라 사회에서의 그의 기능에 관련하여 고려되고 다른 기본권과 균형되어야 한다.[10] 따라서 GDPR은 모든 기본권을 존중하고 사상, 양심과 종교의 자유, 표현과 정보의 자유, '사업 수행의 자유' (freedom to conduct a business) 등 EU기본권헌장에서 인정된 자유와 원칙을 준수한다.[11]

를 보호하고 개인의 존엄과 가치를 구현하는 목적을 가진다고 규정하여, 개인정보의 자유로운 이동이 개인정보보호와 같은 수준에서 중요한 법적 이익이고 가치라는 점을 명시하지 않는다. 개인정보보호법 제1조 참조.

9) EU의 단일디지털시장의 완성이야말로 적어도 EU 내에서 미국의 IT기업들을 능가하려는 취지의 제도이다.

10) GDPR 상설 제4항.

11) GDPR 상설 제4항.

2. 프로파일링에 관한 규정 검토

GDPR의 프로파일링 (profiling) 규정은 데이터 중심의 디지털경제에서 개인정보를 처리하는 기업에 큰 영향을 미칠 것이다. 프로파일링은 개인정보 처리의 법적 근거나 개인정보보호원칙과 같이 개인정보 처리를 규율하는 GDPR 규정의 적용을 받는다.[12] EU 역외에 설립된 한국 기업도 경우에 따라서 GDPR의 프로파일링에 관한 규정의 적용을 받게 된다.[13] GDPR의 가명조치와 목적 외 처리 및 프로파일링 규정은 빅데이터 분석기술을 활성화할 수 있는 법적 장치가 되는데, GDPR은 프로파일링을 포함한 자동화된 처리에만 기초한 의사결정에 따라 정보주체가 피해를 보지 않도록 규정한다. 이렇게 정보주체를 보호하는 규정은 빅데이터 분석기술에 대한 제한이 될 수 있다. GDPR의 프로파일링 규정은 유럽의회, EU이사회와 유럽위원회 사이의 '3자협의'(Trilogue)에서 마지막 단계에서 타결된 쟁점 중의 하나이다.

1995년 지침도 자동화된 의사결정에 관한 규정을 두고 있다. 동 지침 제15조는 GDPR 제22조과 유사하게 '자동화된 개별 결정' (automated individual decisions)을 따르지 않을 정보주체의 권리를 규정하지만, 프로파일링이 자동화된 처리에 포함된다고 명시하지 않는다. 다만, 동 지침이 채택될 당시 인간의 개입 없는 순전한 자동화된 수단에 의한 결정은 일반적이지 않았다. 이후 인터넷에서의 개인정보의 폭넓은 이용가능성과 기술 발전이 빅

12) GDPR 상설 제72항.

13) GDPR의 역외적용을 허용하는 제3(2)조 참조.

데이터 분석기술과 결합하여 프로파일링이 보다 큰 이슈가 되면서 GDPR에 보다 자세한 규정이 마련된 것이다. GDPR은 프로파일링을 이용하는 자동화된 의사결정은 물론 프로파일의 생성 즉, 프로파일링에도 적용된다. 즉, GDPR은 프로파일링의 정의 규정과 함께 프로파일링에 관련된 정보주체의 권리와 컨트롤러의 의무를 규정한다. 이들 권리와 의무는 프로파일링이 수행되는 경우 동 처리의 보다 큰 투명성과 정보주체의 보다 큰 통제를 보장하려고 한다. 1995년 지침과 비교할 때, GDPR은 프로파일링을 별도로 정의하고, 정보주체의 명시적 동의에 따라 프로파일링을 포함한 자동화된 처리에만 기초한 결정에 따를 수 있게 하며, 민감정보에 기초한 자동화된 의사결정을 엄격하게 예외적으로 허용하는 점에서 차이가 있다.

〈자동화된 결정에 관한 1995년 지침과 2016년 GDPR의 비교〉

1995년 지침 제15조 자동화된 개별 결정	GDPR 제22조 프로파일링을 포함한 자동화된 개별 의사결정
1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. 2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision: (a) is taken in the course of the entering into	1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including **profiling**, which produces legal effects concerning him or her or similarly significantly affects him or her. 2. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and

or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.	legitimate interests; or (c) is based on the **data subject's explicit consent**. 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. 4. **Decisions** referred to in paragraph 2 shall **not be based on special categories of personal data** referred to in Article 9(1), **unless** point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

1) 프로파일링의 개념

일반적으로 프로파일링은 개인 또는 개인 그룹에 관한 정보를 수집하고 그의 특성 또는 행태를 분석하여 그(들)를 일정한 범주 또는 그룹에 넣거나 일의 수행 능력, 관심 또는 가능한 행동에 관한 예측 또는 평가를 하는 것을 의미한다.[14] 프로파일링이 개인의 프로파일을 바탕으로 개인들을 특정 그룹

14) UK ICO, *Feedback request - profiling and automated decision-making*, 5-6 (April 2017) (이하 2017 ICO라 함).

으로 분할하는 점에서 의도되지 않은 불합리한 차별이 발생하는 큰 문제가 있다.

행정안전부는 2017년 8월 9일 인공지능 (AI)과 빅데이터, 사물인터넷(IoT) 등 첨단기술을 활용해 공공행정을 혁신하는 '차세대 전자정부'정책을 발표했하였다. 동 정책의 지능형 정부 과제의 예로서 제시된 개인의 주변 상황과 자주 이용하는 서비스 이력을 추력 관리하여 맞춤형 서비스를 제공하기 위하여 비콘, GPS, 상황인지 등을 통하여 개인의 상황을 인식하고, AI, 빅데이터 등을 활용하여 개개인에게 적합한 정보를 제공하는 것은 프로파일링에 기초하게 될 것이다.[15]

GDPR은 프로파일링을 '자연인과 관련된 일정한 개인적 측면을 평가하기 위하여, 특히 그 자연인의 업무능력, 경제 상황, 건강, 개인적 선호, 관심사, 신뢰도, 행동, 위치 또는 이동과 관련된 측면을 분석하거나 예측하기 위하여 개인정보를 사용하는 모든 형태의 자동화된 개인정보 처리'(밑줄 추가)라고 정의한다.[16] 프로파일링은 다음의 세 가지 요소로 구성된다. 첫째, 프로파일링은 개인정보의 '자동화된 처리'이다. 둘째, 프로파일링은 '개인정보'에 대하여 수행되어야 한다. 셋째, 프로파일링은 '자연인에 관한 개인적 측면의 평

15) 행정안전부, "국민의 일상과 함께하는 '지능형 정부' - 행안부, 「4차 산업혁명 대응 전자정부 협의회」 개최 -", 보도자료, 2017.8.9. 참조.

16) GDPR 제4조(4). 동 원문은 다음과 같다: "Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

가', 특히 '분석 또는 예측'을 목적으로 한다.

프로파일링은 예컨대, '어느 웹사이트 방문자의 15%가 여성이고 전문직에 종사하며 20대 중반에서 30대 중반이다'와 같이 분석적이거나 '특정 대출 신청자가 그 대출을 상환하지 않을 위험성이 높다'와 같이 평가적이거나 또는 '이 홍보는 스포츠에 관심 있는 30대 중반에서 40대 중반의 남성을 대상으로 한다'와 같이 표적적인 것과 같이 사람들의 개인정보를 이용하여 그들이 어떤 부류의 사람인지 또는 어떻게 행동하는지를 확인하는 것을 의미한다.[17]

GDPR에서 프로파일링은 '개인정보를 사용하는 모든 형태의 자동화된 개인정보 처리'인 점에서 프로파일링은 자동화된 의사결정의 예가 아니라 자동화된 처리의 예가 된다. 즉, GDPR 제22조의 제목이 '프로파일링을 포함한 자동화된 개별 의사결정' (Automated individual decision-making, including profiling)이어서 프로파일링이 자동화된 의사결정의 한 예가 되는 것으로 보이지만, 동 규정의 내용에서 명시된 대로 프로파일링은 자동화된 처리의 예이다.[18] 컨트롤러는 개인의 프로파일을 이용하여 자동화된 의사결정을 하는 것이어서 프로파일링은 그 자체로서 자동화된 의사결정이 아닌 것이다. 예컨

17) Phil Lee, "Let's sort out this profiling and consent debate once and for all", Privacy, Security and Information Law, July 4, 2017, http://privacylawblog.fieldfisher.com/2017/let-s-sort-out-this-profiling-and-consent-debate-once-and-for-all/.

18) GDPR 제22(1)조는 '프로파일링을 포함한 자동화된 처리' (automated processing, including profiling)이라고 규정한다. GDPR 상설 제71항도 정보주체가 자동화된 처리에만 기초한 결정에 따르지 않을 권리를 가진다고 설명하면서, 그러한 처리, 즉 '자동화된 처리' (automated processing)가 프로파일링을 포함한다고 명시한다.

대, 대출 신청자에게 대출을 할 것인지의 결정을 위하여 그의 신용 프로파일을 이용하는 것이다. 따라서, GDPR 제22조는 프로파일링을 포함한 자동화된 처리에만 기초한 결정에 따르지 않을 정보주체의 권리를 규정한 것이지, 자동화된 처리인 프로파일링 그 자체를 제한하려는 것은 아니다.

GDPR의 적용 범위는 1995년 지침에 비교하여 확대된다. 즉, 전통적인 적용 범위인 EU 내에 설립된 컨트롤러에 더하여 '처리 활동이 ... 그의 [EU 내 정보주체] 행태가 EU 내에서 이루어지는 한 그 의 행태의 감시에 관련되는 경우' (where the processing activities are related to (…) the monitoring of their [data subjects who are in the Union] behaviour as far as their behaviour takes place within the European Union) EU 내에 설립되지 않은 컨트롤러에게도 적용되기 때문이다.[19] 여기서 프로파일링은 GDPR의 역외적용을 확대하는 요소인 정보주체의 행태 감시 (monitoring)의 중요한 요소이다. 즉, 정보주체의 행태 감시로 인정되기 위하여, 개인정보 처리 기술의 잠재적인 추후 이용으로 개인이 인터넷에서 추적되는지 확인되어야 하는데, 이러한 기술은 '특히 그에 관한 결정을 내리기 위하여 또는 그의 개인적 취향, 행태 및 태도를 분석하거나 예측하기 위한 자연인의 프로파일링' (profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes)으로 구성된다.[20] 따라서, EU 역외에 설립되지만

19) GDPR 제3조.

20) GDPR 상설 제24항.

프로파일링의 맥락에서 EU 거주자의 개인정보를 처리하는 기업 등은 GDPR, 특히 프로파일링을 포함한 자동화된 의사결정에 관한 규정의 적용을 받는다. 따라서 EU에서 판매보다 더 넓은 범위의 마케팅 (marketing) 활동을 하는 한국 기업들도 GDPR의 적용을 받을 수 있게 된다.

2) 프로파일링에 대한 개인정보보호 원칙의 적용

개인정보를 처리하는 기관의 입장에서 프로파일링은 해당 정보주체에 관련한 자동적인 예측과 평가의 혜택을 주지만, 정보주체의 입장에서 자신의 개인정보 처리에 관한 권리의 행사에 있어서 위험도 준다.

〈프로파일링의 혜택과 위험〉[21]

혜택	위험
시장의 세분화	정보주체의 기본권과 자유의 침해
위험과 사기의 분석 가능	노년층, 취약계층 또는 소셜미디어가 제한된 사람들과 같은 사회의 일정 부문이 소외될 수 있음
개별 소비자의 수요에 맞춘 상품과 서비스 및 가격의 제공	합리적 수준의 확실성으로 민감하지 않은 개인정보로부터 민감한 개인정보를 추정할 수 있음
의약, 교육, 건강관리 및 교통에서의 개선	상품이나 서비스의 정당화할 수 없는 박탈
전통적 신용평점과 다른 방법을 이용하는 신용에 대한 접근	개인이 모르게 자신의 상업적 이익을 위하여 정보를 이용하는 정보중개산업의 위험
의사결정 과정에서 보다 나은 일관성의 제공	정보의 정확성을 해칠 수 있는 프로파일링 기술의 이용

21) 2017 ICO, p. 6.

개인정보의 처리인 프로파일링은 GDPR이 요구하는 개인정보 처리에 관한 일반원칙의 적용을 받으며, GDPR은 프로파일링에 특별하게 적용되는 규정도 두고 있다.

(1) 처리의 적법성

컨트롤러는 프로파일링 맥락에서 개인정보 처리의 법적 근거를 고민하여야 하는데, 예컨대, 프로파일링이 정보주체의 동의에 근거하는 경우 동의는 '자유롭게 주어지고, 특정되며, 고지되고, 모호하지 않아야'한다.[22] 다만, 프로파일링의 특성에서 이러한 동의의 입증은 쉽지 않을 것이다. 동의 이외에 다음과 같은 법적 근거가 프로파일링에 이용될 것이다:[23] 계약의 이행에 필요한 경우; 또는 컨트롤러 또는 제3자가 추구하는 정당한 이익의 목적에 필요한 경우. 이러한 두 가지 법적 근거를 충족하기 위하여 프로파일링은 각각의 목적 충족에 '필요한' (necessary) 점을 입증할 수 있어야 한다.

프로파일은 정보주체가 직접 제공한 개인정보가 아닌 파생되거나 추론된 정보로 구성되는 경향이 있다.[24] 프로파일링의 결과로서 컨트롤러는 정보주체의 민감정보를 식별하게 될 수도 있다.[25] 예컨대, 개인의 식품 구매 기록

22) GDPR 제4조(11). 민감정보에 대한 동의는 '명시적' (explicit)이어야 한다. GDPR 제9(2)조(a).

23) 2017 ICO, p. 13. 각각 GDPR 제6(1)조(b) 및 제6(1)조(f) 참조. 이들 두 경우는 민감정보 처리의 법적 근거가 되지 않는다.

24) 2017 ICO, p. 13.

을 개인정보가 아닌 식품의 에너지량과 결합하여 그의 건강상태, 즉 민감정보를 추론할 수 있게 된다. 민감정보에 기초한 자동화된 의사결정은 해당 정보주체의 명시적 동의 또는 회원국이나 EU의 법에 따라서만 허용된다.[26]

(2) 처리의 투명성

GDPR은 다음과 같이 컨트롤러의 프로파일링에 관하여 정보주체에게 '공정한 처리에 관한 정보' (fair processing information)를 제공하도록 요구한다. 이러한 정보주체의 투명한 처리에 대한 권리를 통하여 자동적 의사결정에서의 인간의 개입 요구가 가능해진다.[27] 첫째, 개인정보가 정보주체로부터 직접 수집되거나 그렇지 않은 경우 컨트롤러는 정보주체에게 일정한 정보를 제공해야 한다. 정보주체에 관한 법적 효력을 주거나 그에게 유사하게 중대하게 영향을 미치는 프로파일링을 포함한 자동화된 처리에만 기초한 결정이 이루어지는 경우 '프로파일링을 포함한 자동화된 의사결정의 존재 ... 및 ... 정보주체에 대한 이러한 처리의 중요성과 예견된 결과와 함께 수반된 로직에 관한 의미있는 정보'(the existence of automated decision-making, including profiling ... and, ... meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject)가 이렇게 정보주체에게 제공되는 정보에 포함된다.[28] 컨트롤러는 정보주체로부터 직접 개인정보를 수집하는 경

25) 2017 ICO, p. 13.

26) GDPR 제22(4)조.

27) GDPR 제22(3)조 참조.

28) 각각 GDPR 제13(2)(f)조와 제14(2)(g)조.

우 동 개인정보가 획득되는 시점에서, 및 동 개인정보가 정보주체로부터 직접 획득되지 않는 경우 동 개인정보의 획득 후 합리적 기간 내에 위의 프로파일링에 관한 정보를 제공해야 한다.[29] 또한, 컨트롤러는 개인정보가 처리되는 특정 상황과 문맥을 고려하여 공정하고 투명한 처리를 보장하는데 필요한 '어떠한 추가적 정보' (any further information)라도 정보주체에게 제공해야 한다.[30] 따라서 상황에 따라서 컨트롤러는 정보주체에게 프로파일링에 관한'존재', '중요성', '예견된 결과' 및 '로직에 관한 의미있는 정보'가 아닌 추가적 정보를 제공해야할 수도 있다.

둘째, 정보주체는 컨트롤러로부터 자신에 관한 개인정보가 처리되고 있는지의 확인을 요구할 권리를 가진다. 정보주체에 관한 법적 효력을 주거나 그에게 유사하게 중대하게 영향을 미치는 프로파일링을 포함한 자동화된 처리에만 기초한 결정이 이루어지는 경우 '프로파일링을 포함한 자동화된 의사결정의 존재 ... 및 ... 정보주체에 대한 이러한 처리의 중요성과 예견된 결과와 함께 수반된 로직에 관한 의미있는 정보'에 대하여 정보주체는 접근권 (right of access)을 가진다.[31] 컨트롤러는 이러한 정보를 간결하고, 투명하며, 이해할 수 있고, 쉽게 접근할 수 있는 형식으로, 특히 아동을 특정적으로 대상으로 한 정보에 대하여는 명확하고 평이한 언어를 사용하여 제공할 적절한 조치를 취해야 한다.[32]

---

29) 각각 GDPR 제13(2)조 및 제14(3)(a)조.

30) GDPR 상설 제60항. 여기서 'should'가 사용되어 이러한 추가적 정보의 제공은 법적으로 강제된 것은 아니다.

31) GDPR 제15(1)(h)조.

정보주체의 접근권 행사의 결과 모든 정보주체는 자동화된 개인정보 처리에 수반된 로직 및 적어도 프로파일링에 기초한 경우 그러한 처리의 결과를 알 권리를 가진다.[33] 그러나, 정보주체의 이러한 권리는 영업비밀이나 지재권 및 특히 소프트웨어를 보호하는 저작권을 포함한 다른 자들의 권리나 자유에는 부정적인 영향을 미치지 않아야 한다.[34]. 따라서 프로파일링과 관련한 로직을 실행하는 알고리즘의 세부사항은 정보주체에게 공개되지 않을 것이다.

(3) 처리에 대한 반대권

정보주체는 컨트롤러의 개인정보 처리에 대한 반대권을 행사할 수 있는데, GDPR은 이러한 개인정보 처리에 프로파일링을 명시한다. 첫째, 정보주체는 다음의 두 가지 법적 근거에 따른 프로파일링을 자신의 특별한 상황에 관한 사유로 언제든지 반대할 권리를 가져야 한다:[35] 1). 공익을 위하여 수행되는 직무의 실행을 위하여 또는 컨트롤러에게 부여된 공적 권한의 행사에 처리가 필요한 경우; 2). 컨트롤러나 제3자가 추구하는 정당한 이익의 목적을 위하여 처리가 필요한 경우로서, 다만, 특히 정보주체가 아동인 경우와 같이 개인정보 보호를 요구하는 정보주체의 이익이나 기본권과 자유가 해당 이익에

32) GDPR 제12(1)조.

33) GDPR 상설 제63항.

34) GDPR 상설 제63항.

35) GDPR 제21(1)조 제1문. 이들 두 적법한 처리의 근거는 각각 GDPR 제6(1)(e)조 및 제6(1)(f)조 참조.

우선하는 경우에는 그러하지 아니하다. 컨트롤러는 정보주체의 이익, 권리 및 자유에 우선하는 처리 또는 법적 청구권의 설정, 행사 또는 방어를 위한 '납득할만한 정당한 근거' (compelling legitimate grounds)를 입증하지 않는 한 프로파일링을 더 이상 수행하지 말아야 한다.[36] 따라서 정보주체의 프로파일링에 대한 반대권의 행사에 컨트롤러와 정보주체의 이익 사이의 비교 평가가 이루어져야 한다. 컨트롤러의 납득할 만한 정당한 근거의 입증은 컨트롤러가 부담한다.[37]

둘째, 직접 마케팅을 목적으로 개인정보가 처리되는 경우, 정보주체는 언제든지 이러한 마케팅을 위한 자신에 관한 개인정보 처리에 반대할 권리를 가져야 하고, 이러한 직접 마케팅과 관련되는 한도 내에서 프로파일링을 포함한다.[38] 정보주체가 직접 마케팅에 관련되는 한도에서 프로파일링에 반대하는 경우, 개인정보는 더 이상 그러한 목적으로 처리되어서는 안 된다.[39] 직접 마케팅에 관련된 프로파일링에 대한 반대권의 행사는 절대적이다.

(4) 프로파일링을 포함한 자동화된 처리에만 기초한 결정에 따르지 않을 권리

GDPR 제22조는 프로파일링을 포함한 개인에 대한 자동적 의사결정을 다음과 같이 규정하는데, 프로파일링을 정의하는 제4조(4)와 함께 프로파일링

36) GDPR 제21(1)조 제2문.

37) 2017 ICO, p. 17.

38) GDPR 제21(2)조.

39) GDPR 제21(3)조.

에 관한 특별한 규정이다. 우선, 정보주체는 자신에 관한 법적 효력을 주거나 자신에게 유사하게 중대하게 영향을 미치는 '프로파일링을 포함한 자동화된 처리에만 기초한 결정' (a decision based solely on automated processing, including profiling)에 따르지 않을 권리를 가진다.[40] 프로파일링을 포함한 자동화된 처리에'만' (solely)의 의미는 사람이 그 결정의 결과에 대하여 실제적인 영향을 주지 않는 경우, 즉 그 결정이 내려지기 전에 사람의 평가가 없는 경우를 말할 것이다.[41] 또한, 정보주체는 공식적인 결정은 물론 법적 효력을 주거나 유사하게 중대하게 영향을 미치는 '조치' (measures)로부터도 보호를 받는다.[42] 예컨대, 인터넷에서 개인의 검색에 기초한 특정 항암제의 표적 마케팅은 이러한 조치에 해당한다.[43]

이렇게 자동화된 의사결정에 따르지 않을 권리는 일반적으로 이러한 처리에 반대할 권리로 해석된다. 따라서 실제에 있어서는 정보주체에게 법적 효력을 주거나 이와 유사하게 중대한 영향을 주는 프로파일링에 그 정보주체의 동의가 필요할 것이다. 다만, GDPR은 '법적 효력'(legal effects)과 '유사하게 중대하게 영향을 미치는'(similarly significantly affects)의 개념을 설명하지 않는다. 법적 효력은 개인의 법적 권리나 그의 법적 신분에 부정적으로 영향을 주는 것으로 볼 수 있고, 유사하게 중대하게 영향을 미치는 것은 사소하

---

40) GDPR 제22(1)조.

41) 2017 ICO, p. 19.

42) GDPR 상설 제71항

43) Viviane Reding, "The EU data protection Regulation: Promoting technological innovation and safeguarding citizens' rights", 4 March 2014, http://europa.eu/rapid/press-release_SPEECH-14175_en.htm?locale=en.

지 않고 부정적 영향을 가지는 결과를 가리킬 것이다.[44] 정보주체가 반대할 수 있는 프로파일링의 실제적 확인은 각각의 회원국 감독당국과 법원의 결정으로 다를 수 있지만, 컨트롤러나 정보주체의 주관적 견해에 따르지 않고 객관적으로 인정된 기준을 확립하는 것이 바람직할 것이다. 다만, GDPR은 '인간의 개입 없이 온라인 신용거래신청이나 전자적 채용의 자동적 거절'을 개인에게 법적 효력 또는 중대한 영향을 주는 자동화된 처리의 예로서 제시한다.[45]

그러나, 프로파일링을 포함한 자동화된 처리에만 기초한 결정이 다음의 세 가지 경우의 하나에 해당하면 정보주체의 동 결정에 따르지 않을 권리가 인정되지 않는다.[46] 첫째, 정보주체와 컨트롤러 간에 계약을 체결하거나 이행하기 위하여 필요한 경우이다.[47] 둘째, 컨트롤러가 준수하여야 하고 정보주체의 권리와 자유 및 정당한 이익을 보호하기 위한 적합한 조치를 규정하고 있는 EU 또는 회원국의 법에 의해서 허용된 경우이다.[48] EU기관이나 회원국 국내감독기구의 규정, 기준 및 권고에 따라 수행되는 기망과 탈세 감시 및 예방 목적 및 컨트롤러가 제공하는 서비스의 안전과 신뢰성을 보장할 목적의 결정이 그 예이다.[49] EU 또는 회원국 법으로 부과될 수 있는 프로파일링에 기초한 결정에 대한 제한은 공공안전 등을 보호하기 위하여 민주사회에

---

44) 2017 ICO, p. 19.

45) GDPR 상설 제71항.

46) 유럽개인정보보호이사회(European Data Protection Board)는 프로파일링에 기초한 자동적 의사결정을 위한 기준과 조건을 한층 더 구체화하는 가이드라인, 권고 및 모범관행을 공표해야 한다. GDPR 제70(1)(f)조 및 상설 제72항.

47) GDPR 제22(2)(a)조.

48) GDPR 제22(2)(b)조.

49) GDPR 상설 제71항.

서 필요하고 비례적이면 부과될 수 있다.[50] 셋째, 정보주체의 명시적인 동의에 근거한 경우이다.[51]

특히 위의 첫째와 셋째의 경우, 즉 정보주체와의 계약 관계나 그의 명시적 동의에 근거하여 프로파일링이 허용되면, 컨트롤러는 정보주체가 자신의 의견을 표시하고 그 결정에 이의를 제기하기 위하여 자신의 권리와 자유 및 정당한 이익, 최소한 컨트롤러의 '인적 개입' (human intervention)을 획득할 권리를 보장하기 위한 적합한 안전장치를 이행하여야 한다.[52] 문제는 이러한 인적 개입이 어떻게 이루어질지 명확하지 않은 점이다.

정보주체에 관하여 공정하고 투명한 처리를 보장하기 위하여, 개인정보가 처리되는 특정된 상황과 맥락을 고려하여, 컨트롤러는 첫째, 프로파일링을 위한 적절한 수학적 또는 통계적 절차를 이용하고, 둘째, 특히 개인정보의 부정확성을 초래하는 요소가 시정되고 오류의 위험이 최소화되는 것을 보장할 적절한 기술적 및 관리적 조치를 이행하여야 하며, 셋째, 정보주체의 이익과 권리를 위하여 수반된 잠재적 위험을 고려하고 인종적 또는 민족적 기원, 정치적 의견, 종교 또는 믿음, 노동조합 가입, 유전 또는 건강 지위 또는 성적 지향성에 근거한 자연인에 대한 차별적 효과 등 또는 그러한 효과를 가지는 조치를 금지하는 방식으로 개인정보를 보호하여야 한다.[53]

---

50) GDPR 상설 제73항.

51) GDPR 제22(2)(c)조.

52) GDPR 제22(3)조.

53) GDPR 상설 제71항. 여기서 'should'가 사용되어 법적 강제성은 없다.

(5) 개인정보보호 영향평가

특히 새로운 기술을 이용하는 처리의 한 유형이, 그 처리의 성격, 범위, 맥락 및 목적을 고려할 때, 자연인의 권리와 자유에 대한 '중대한 위험'(a high risk)을 초래할 것 같으면, 컨트롤러는, 해당 처리를 하기 전에, 개인정보 보호에 대한 예상되는 처리작업의 영향평가를 수행해야 한다.[54] 이러한 '개인정보보호 영향평가' (data protection impact assessment)는 프로파일링을 포함한 자동화된 처리에 기초한 '자연인에 관련된 개인적 측면에 대한 체계적이고 폭넓은 평가'(a systematic and extensive evaluation of personal aspects relating to natural persons)이면서, 해당 자연인에 관한 법적 효력을 발생시키거나 이와 유사하게 동 자연인에게 중대한 영향을 미치는 결정의 기초가 되는 경우에 요구된다.[55] 프로파일링에 관한 기본 규정인 GDPR 제22(1)조와 다르게 제35(3)(a)조에서 영향평가가 요구되는 체계적이고 폭넓은 평가는 프로파일링을 포함한 자동화된 처리에 기초하면 되는 것이지, 이러한 처리에만 기초하도록 요구되지 않는다.[56] 따라서 부분적으로 자동화된 처리의 경우에도 영향평가가 요구될 것이다.[57]

개인정보보호 영향평가가 요구되는 프로파일링의 예는 다음과 같다:[58] 신

54) GDPR 제35(1)조.

55) GDPR 제35(3)(a)조.

56) GDPR 제35(3)(a)조는 'based on automated processing, including profiling'이라고 규정하고, 제22(1)조는 'based solely on automated processing, including profiling'이라고 규정하여, 제35(3)(a)조에 'solely'가 빠져 있다.

57) 2017 ICO, p. 22.

58) 2017 ICO, p. 21.

용평가, 보험료 책정, 사기 방지, 돈세탁 탐지 등의 위험 평가 목적의 프로파일링; 모바일 앱 등으로 '푸시 알림' (push notification)을 보낼지 결정을 위한 위치 추적; 로열티 프로그램; 행태 광고; 및 웨어러블 장치를 통한 건강정보 등의 감시.

(6) 아동과 프로파일링

아동은 자신의 개인정보에 관하여 특정 보호를 받아야 하는데, 아동은 관련 위험, 결과 및 안전장치 및 개인정보 처리에 관련한 그의 권리를 덜 이해하기 때문이다. 이러한 특정 보호는 특히 마케팅이나 퍼스낼러티 또는 이용자 프로파일의 생성 목적이나 아동에게 직접 제공되는 서비스의 이용에서 아동에 관한 개인정보의 수집을 위한 아동의 개인정보 이용에 적용된다.[59] 컨트롤러는 아동에게 법적 효과 또는 이와 유사하게 중대한 영향을 주는 프로파일링을 포함한 자동화된 처리에만 기초한 결정을 할 수 없다.[60] 또한, 컨트롤러는 정보주체로부터 직접 개인정보를 수집하거나 그렇지 않은 경우에 프로파일링에 관련된 정보 등을 정보주체에게 제공하여야 하는데, 이러한 정보를 간결하고, 투명하며, 이해할 수 있고, 쉽게 접근할 수 있는 형식으로, 특히 아동을 특정적으로 대상으로 한 정보에 대하여는 명확하고 평이한 언어를 사용하여 제공할 적절한 조치를 취해야 한다.[61]

59) GDPR 상설 제38항.

60) GDPR 상설 제71항.

61) GDPR 제12(1)조.

3) 민감정보의 프로파일링

위에서 허용된 세 가지 경우의 프로파일링을 포함한 자동화된 처리에만 기초한 결정이 특수한 범주, 즉 민감정보에 기초하기 위하여, 정보주체의 명시적 동의가 있거나 EU나 회원국 법에 근거하여 중대한 공익을 이유로 개인정보 처리가 필요한 경우로서 정보주체의 권리와 자유 및 정당한 이익을 보장할 적합한 안전장치가 마련되어야 한다.[62]

정보주체에 관하여 공정하고 투명한 처리를 보장하기 위하여, 개인정보가 처리되는 특정된 상황과 맥락을 고려하여, 컨트롤러는 첫째, 프로파일링을 위한 적절한 수학적 또는 통계적 절차를 이용하고, 둘째, 특히 개인정보의 부정확성을 초래하는 요소가 시정되고 오류의 위험이 최소화되는 것을 보장할 적절한 기술적 및 관리적 조치를 이행하여야 하며, 셋째, 정보주체의 이익과 권리를 위하여 수반된 잠재적 위험을 고려하고 인종적 또는 민족적 기원, 정치적 의견, 종교 또는 믿음, 노동조합 가입, 유전 또는 건강 지위 또는 성적 지향성에 근거한 자연인에 대한 차별적 효과 등 또는 그러한 효과를 가지는 조치를 금지하는 방식으로 개인정보를 보호하여야 한다.[63]

4) 벌칙

62) GDPR 제22(4)조.

63) GDPR 상설 제71항.

프로파일링을 포함한 자동화된 의사결정에 관하여 정보주체의 권리가 침해되면, 2천만 유로 이하 또는 사업체인 경우 이것과 직전 회계연도의 전세계 연간 총매출액의 4% 이하 중 높은 금액으로 과징금이 부과된다.[64] 벌칙은 컨트롤러 등의 GDPR 준수를 도모하기 위한 다양한 수단의 하나이어서, GDPR 위반에 대하여 비례성과 신중함에 따라, 이러한 벌칙의 최대치가 항상 적용되지는 않을 것이라고 한다.

3. 결론

자동화된 의사결정에 관하여 GDPR은 1995년 지침과 유사한 제한을 두지만, 다음과 같은 중요한 변경을 도입한다. 첫째, 프로파일링의 개념이 정의되고, 둘째, 정보주체의 명시적 동의가 프로파일링을 포함한 자동화된 처리에만 기초한 결정을 허용하는 새로운 법적 근거가 되며, 셋째, 민감정보에 기초한 프로파일링을 포함한 자동화된 처리에만 기초한 결정을 예외적으로 허용하고, 넷째, 컨트롤러는 정보주체에게 프로파일링에 관한 정보를 고지할 의무를 가진다.

개인정보보호법은 프로파일링을 포함한 개인정보의 자동화된 처리 및 이에 기초한 결정을 명시적으로 제한하는 규정을 두지 않는다. 소위 인공지능(AI) 기술의 활성화로 개인정보의 자동화된 의사결정이 활성화됨에 따라 개

64) GDPR 제83(5)조.

인정보보호 차원에서 정보주체와 개인정보처리자의 이익이 균형되도록 이에 대한 명시적 규정이 도입되어야 할 것이다. 이 점에서 GDPR이 좋은 선례가 될 수 있다.

메모

메모

메모

메모