발 간 등 록 번 호
11- 1620000- 000800- 01

2020년도 일반과제 실태조사
연구용역보고서

유럽연합「개인정보보호 규정」(GDPR) 등 국제인권기준에 따른 개인정보 보호 법제도 개선방안 연구

국가인권위원회

Nation Human Rights Commission of Korea

발 간 등 록 번 호
11- 1620000- 000800- 01

2020년도 일반과제 실태조사
연구용역보고서

유럽연합「개인정보보호 규정」(GDPR) 등 국제인권기준에 따른 개인정보 보호 법제도 개선방안 연구

국가인권위원회

Nation Human Rights Commission of Korea

유럽연합「개인정보보호 규정」(GDPR) 등 국제인권기준에 따른 개인정보 보호 법제도 개선방안 연구

2020년도 국가인권위원회 일반과제 실태조사
연구용역 최종보고서를 제출합니다.

2020. 11. 16.

연구수행기관 : 사단법인 정보인권연구소
연구책임자 : 이호중 (사단법인 정보인권연구소 이사장)
공동연구원 : 이은우 (사단법인 정보인권연구소 이사)
오병일 (사단법인 정보인권연구소 연구위원)
장여경 (사단법인 정보인권연구소 이사)
김재완 (법학박사)
보조연구원 : 정선화 (진보네트워크센터 활동가)

이 보고서는 연구용역수행기관의 결과물로서,
국가인권위원회의 입장과 다를 수 있습니다.

목 차

〈표 차례〉

<그림 차례>

요 약 문

제1장 서론

제1절 연구 목적 및 필요성

세계 각국은 새로운 기술과 서비스 개발에 필요한 개인정보의 안전한 활용을 촉진하면서도, 증가하는 개인정보 침해 위협에 대응하기 위한 법제의 개편을 시도하고 있다. 대표적인 것이 유럽연합의 일반개인정보보호규정(GDPR)이다. 유럽평의회가 1981년 채택한 <개인정보의 자동처리와 관련된 개인의 보호를 위한 유럽회의 협약>, 즉 108호 협약은 개인정보 보호를 위한 구속력 있는 유일한 국제협약이다.

한국 정부 역시 2010년대 초반부터 빅데이터 등 신기술 발전에 대응하여 개인정보 보호 규범의 변화를 도모해왔다. 그러나 그 방향은 주로 빅데이터 산업 활성화를 명분으로 개인정보 보호를 완화하는 것에 맞추어졌다. 소위 데이터 3법이 2020년 1월 9일 국회를 통과하여 같은 해 8월 5일 시행되었다. 데이터 3법의 주요 내용은 크게 두 가지이다. 첫째는 정보주체의 동의 없이 과학적 연구, 통계작성, 공익적 기록보존 등의 목적으로 가명정보를 이용할 수 있는 근거를 마련하는 것, 둘째는 개인정보의 오용·남용 및 유출 등을 감독할 감독기구는 개인정보 보호위원회로, 관련 법률의 유사·중복 규정은 개인정보 보호법으로 일원화하는 방향으로 법제를 체계적으로 정비하는 것이다.

본 연구는 빅데이터와 인공지능 등 신기술 환경에서 개인정보 자기결정권을 보호하기 위한 국내 법제도 개선방안의 도출을 목적으로 한다. GDPR, 108+ 협약, OECD 및 유엔 가이드라인 등 개인정보 보호 국제규범에 대한 면밀한 검토와 국내 법제와의 비교 분석을 통해 국내 법제에서 도입이 필요한 이슈들을 도출하고 국내 환경에서 어떻게 도입하면 좋을지 적절한 방안을 권고하고자 한다.

개인정보 보호위원회와 국가인권위원회 사이의 역할 정립도 필요하다. 특히 인공지능이 인권에 미치는 영향은 비단 개인정보 문제에 국한하지 않고 표현의 자유, 차별 등 인권 전반에 폭넓게 미치는 만큼 국가인권위원회가 해야 할 역할이 크다.

제2절 연구내용 및 범위

본 연구는 우선 제2장에서 빅데이터, 인공지능 등 신기술의 발전에 대응하여 OECD, 유럽연합, 미국 및 일본 등 세계 각국의 개인정보 규범이 최근 몇 년 동안 어떻게 변화하였는지를 중심으로 살펴보았다. 제3장에서는 국내 개인정보 보호 법제를 둘러싼 최근 과제를 다루었다. 데이터 3법을 둘러싼 논란을 검토하고 향후 개인정보 보호 법제를 어떻게 개선해야 하는지 큰 방향을 제시하고자 하였다. 이와 같은 국내외 현황 분석과 개선 방향을 토대로, 제4장부터는 중요한 이슈별로 구체적인 개선방안을 검토하였다. 개선방안은 크게 정보주체의 권리보호 강화 방안(제4장), 개인정보처리자의 책임성 강화 방안(제5장), 범죄예방 및 수사 등 분야에서 개인정보 보호 방안(제6장)으로 구분하였다.

제4장에서는 열람권 등 기존 정보주체의 권리들을 GDPR 및 미국 캘리포니아 소비자 프라이버시 보호법(CCPA) 등의 내용과 비교하면서 개선방안을 제시하였다. 또한 국내에서도 실효성 논란이 제기되고 있는 동의 제도가 어떻게 개선되어야 하는지 살펴보았다.

제5장에서는 해외 규범을 참고하여 개인정보 영향평가, 설계 및 기본설정에 의한 개인정보 보호 등 개인정보처리자의 책임성을 강화하기 위한 다양한 제도를 분석하였다. 제6장은 범죄예방과 수사 등 분야에서 개인정보 보호 이슈를 다루었는데, 유럽연합의 경찰 디렉티브의 주요 내용을 검토하고 국내 법제의 개선방안에 대해 제안하였다.

제7장에서는 개인정보 보호 분야에서 국가인권기구와 개인정보 감독기관의 역할을 분석하고, 상호 역할 분담 및 협력하는 국내외 사례를 검토하면서 향후 국가인권기구가 해야 할 역할을 제안하였다. 마지막 제8장에서는 연구의 결론과 함께, 향후 구체적인 정책 및 입법이 되어야 할 사항들을 정책권고로 제안하였다.

제2장 신기술 발전과 세계 개인정보 보호 규범의 변화

제1절 유엔 등 국제기구의 개인정보 보호 규범

각국의 개인정보 보호 법제의 형성에 지대한 영향을 미친 최초의 국제 규범으로 1980년에 경제협력개발기구(OECD)가 작성한 <프라이버시 보호와 개인정보의 국제유통에 대

한 가이드라인(일명 'OECD 프라이버시 가이드라인')>도 자동화된 개인정보처리의 발전과 방대한 개인정보들의 국경을 넘는 유통을 배경으로 한다. 그 이후 빅데이터, 사물인터넷, 인공지능 등 신기술이 급속하게 발전하고 있으며, 인터넷과 모바일 기기의 확산으로 전 세계 이용자를 대상으로 한 상품과 서비스의 세계적인 유통이 활성화되면서 개인정보를 수집, 처리하는 방식도 국경을 넘어 계속 달라지고 있다. 개인정보 보호 규범도 이러한 기술, 사회, 경제적 환경의 변화에 대응하여 발전하고 있으며, 각 국의 서로 다른 규범이 통일화되는 경향도 강화되고 있다.

OECD의 2013년 가이드라인은 기존의 가이드라인에 비하여 위험 관리에 기반한 접근을 통한 프라이버시 보호의 실질적인 이행, 상호운용성 증진을 통한 국제적인 차원의 프라이버시 대응 노력의 필요성이 보강되었는데 특히 개인정보처리자의 '책무성 이행'이 새롭게 추가되었다.

유엔은 특히 2013년 에드워드 스노든이 정보기관에 의한 인터넷 대량 감시를 폭로한 이후, 총회 및 인권이사회의 반복적인 결의안을 통해 독립적인 감독을 비롯하여 디지털 시대 프라이버시 보호를 위한 적절한 조치를 취할 것을 각국 정부에 촉구하고 있다. 2015년 3월 26일 유엔 인권이사회는 프라이버시 특별보고관을 신설하였으며, 첫번째 특별보고관으로 임명된 조셉 카나타치는 2019년 7월 한국을 공식 방문하여 프라이버시 보호 실태를 조사하였다.

1981년에 유럽평의회가 체결한 <개인정보의 자동화된 처리에 관한 개인의 보호를 위한 협약>(일명 '108호 협약')은 개인정보 분야에서 유일하게 법적으로 구속력있는 국제협약으로 남아있다. 2001년에는 108호 협약의 추가 의정서가 채택이 되었는데, 비회원국인 제3국으로의 개인정보 이전 문제, 국가 개인정보 감독기관의 의무적 설립 문제를 다루고 있다. 이후 추진된 108호 현대화 협약은 추가 의정서의 규정들을 흡수하고, 새로운 정보통신기술의 활용에 따른 문제들에 대응하는 한편으로 협약의 효과적인 이행을 강화하는데 그 목표를 두었다.

제2절 주요 국가의 개인정보 보호 법제

1. 유럽연합

가. 유럽연합의 개인정보 보호법제

유럽연합의 주요 개인정보 보호법제로는 우선 1995년 10월 채택된 개인정보보호 디렉티브(95/46/EC)가 기존 각 국의 법률과 유럽평의회 108호 협약을 기본으로 하면서, 이를 확대하였다. 특히 개인정보 보호 규범에 대한 준수를 강화하기 위해 독립적인 감독기관을 도입했는데, 이는 2001년에 108호 협약 추가 의정서 채택에 영향을 주었다. 이처럼 유럽연합과 유럽평의회의 규범들은 상호 작용을 하면서 긍정적인 영향을 미치고 있다. 그러나 유럽연합의 지침은 직접적인 효력을 가지는 것이 아니라 회원국의 국내법에 반영이 되어야 한다. 이에 따라 개인정보보호 디렉티브가 회원국 간의 법제 조화를 목표로 했음에도 불구하고, 실제로는 회원국 사이에 서로 다른 방식으로 법제화되었다. 집행이나 제재의 수준도 나라마다 편차가 있었다. 한편, 90년대 중반 이후 정보통신기술은 상당한 발전을 이루었고 개인정보 보호 규범에도 이러한 변화를 반영할 필요성이 제기되었다. 이러한 개혁의 요구들이 2016년 4월 일반개인정보보호규정(GDPR)의 채택으로 이어졌다. GDPR은 2년 동안의 준비 기간을 거쳐 2018년 5월 25일 발효 되었다.

또한 유럽연합의 개인정보보호 디렉티브가 경찰 및 형사사법분야에 적용되지 않았던 문제를 개선하여 2016년에 '경찰 및 형사사법당국을 위한 디렉티브(Directive 2016/680)' (일명 '경찰 디렉티브')가 의결되어 2018년 5월 GDPR과 함께 발효 되었다. 한편 유럽연합은 전자통신분야에 특화된 디렉티브로 2002년 채택된 '프라이버시 및 전자통신에 관한 지(혹은 e-Privacy 디렉티브)' 을 가지고 있다(Directive 2002/58/EC). 2017년 1월, 유럽연합 집행위원회는 e-Privacy 디렉티브를 대체하는 새로운 e-Privacy 규정안을 채택하였다. GDPR이 유럽연합 기본권 헌장 제8조(개인정보보호)를 주로 규율한다면, e-Privacy 규정은 기본권 헌장 제7조(사생활존중권)를 유럽연합 법체계에 통합하려는 것이다. 이 규정은 이전 지침의 규정을 신기술 및 시장 현실에 적용하고 포괄적이며 GDPR과 일관된 체계를 수립하고자 한다.

나. 일반개인정보보호규정(GDPR)

개인정보보호 디렉티브와 달리 GDPR은 회원국의 국내법을 통하지 않고 직접적으로 적용된다. 물론 GDPR 채택 이후 유럽연합 각국은 자국의 개인정보 보호법을 개정하였는데, 이는 한편으로는 GDPR과의 일관성을 유지하면서도 다른 한편으로는 GDPR에서 허용하고 있는 범위 내에서 각국의 재량에 따른 규범을 도입하기 위한 것이다. GDPR이 기존의 규범과 달라지는 주요 특징들은 다음과 같다.

첫째, GDPR의 제정 목적 중의 하나가 '디지털 단일시장에 적합한 통일되고 단순화된 프레임워크'를 구축하고자 한 것인데, 이를 위해 원스탑샵 메커니즘(One-Stop-Shop mechanism)을 도입하였다. 둘째, GDPR은 정보주체의 권리를 강화하였다. 개인정보의 정의는 기존 디렉티브와 크게 달라지지 않았지만, IP 주소와 같은 온라인 식별자(online identifier)를 개인정보 정의 규정에 명시하였고, 생체인식정보와 유전정보를 민감정보에 포함하였다. 자유롭게 주어지고, 특정되며, 정보에 기반(freely given, specific and informed)하도록 한 기존 동의의 정의에 모호하지 않아야 한다(unambigous)는 조건이 추가되었고, 제7조에서 유효한 동의의 요건, 제8조에서는 정보사회 서비스와 관련하여 아동의 동의가 유효하기 위한 조건을 상세하게 규정하였다. 이전 지침에서 규정되어 있었던 정보주체의 권리로서 삭제권과 열람권도 보다 세부적으로 규정되었으며, 새로운 정보주체의 권리로서 개인정보 이동권(right to data portability)이 추가되었다. 셋째, 컨트롤러의 책임성을 강화하기 위하여 새롭게 강화된 조치들이 도입되었다. 우선 개인정보 보호와 관련하여 컨트롤러를 자문하고 감독하는 지위를 가진 DPO(Data Protection Officer)를 도입하였고, 컨트롤러에게 침해 위험이 큰 처리 활동에 대해서 개인정보 영향평가를 수행하도록 하고, 설계 및 기본설정에 의한 개인정보 보호를 일반 의무로 부여하는 한편, 개인정보 처리활동에 대한 기록을 유지하도록 하였다. 넷째, 위험성이 큰 개인정보 침해사고가 발생한 경우, 감독기관 및 정보주체에게 통지하도록 하는 개인정보 침해통지 제도도 확대하였고, 규범위반에 대한 제재도 강화하였다. 기존 디렉티브와 달리 GDPR에서 정보주체는 컨트롤러 뿐만 아니라 프로세서에게도 보상을 요구할 수 있다. 또한 디렉티브와 달리 GDPR은 권리 침해에 대한 사법적 구제를 정보주체의 '권리'로 규정하고 있다. 개인정보 감독기관의 위상과 권한도 기존 디렉티브에 비해 더욱 상세하게 규정하고 있다. 다섯째, GDPR은 사실상 전 세계에 영향을 미치는 국제규범이 되고 있다. 유럽

연합 시민의 개인정보를 처리하는 전 세계 기업 및 기관도 GDPR을 준수해야 하고, 유럽연합 시민의 개인정보가 역외의 제3국으로 이전될 경우 적정성 결정 등 다양한 제도를 적용받기 때문이다.

다. GDPR 시행 2년의 평가

2020년 유럽연합 집행위원회는 GDPR에 대한 첫번째 평가를 수행하고 그 보고서를 공개하였다. 집행위원회는 우선 GDPR이 디지털 전환과 그린 뉴딜을 위한 여러 사업들의 기반이라는 점을 강조하고 있다. 신기술 환경에서 개인정보 보호 규범에 대한 정립과 신뢰가 없다면 디지털 경제의 발전도 불가능하기 때문이다. GDPR 시행과 관련해서는 2년의 기간은 아직 어떤 확고한 결론을 내리기에는 이른 시점이지만, 개선이 필요한 점이 있음에도 불구하고 GDPR 제정 목적을 달성했다는 것이 대체적인 견해라고 평가했다.

첫째, 우선 GDPR 집행 측면에서는 감독기관들이 경고, 질책(reprimand), 과징금(fines), 임시적/최종적 처리 제한 등 강화된 자신의 권한을 균형있게 사용해왔다고 평가했다. 침해의 정도에 따라 과징금의 경우 수천 유로에서 수백만 유로가 부과되기도 했다. 반면 시민단체 엑세스 나우는 2019년 GDPR 집행 활동이 급증하기는 했지만, 진정건수에 비해 낮은 수준의 과징금 부과 건수 등 시장과 이용자가 그 영향력을 느끼기에는 아직 부족하다고 평가했다. 둘째, 협력 및 일관성 메커니즘 측면에서는 감독기관들이 주로 거대 기술기업과 관련된 다국적인 문제에서 원스탑샵 메커니즘(60조) 및 상호 지원(61조)을 통해 협력을 발전시켜왔다고 긍정적으로 평가하였다. 그러나 국경간 분쟁의 효과적인 처리를 위한 절차나 관행의 차이 해소 등 개선이 필요하다는 평가이다. GDPR의 일관된 적용(일관성 메커니즘)을 위해서는 EDPB의 역할이 중요하다. 2019년 12월까지 EDPB는 제64(1)조에 따른 의견서를 36개, 제64(2)조에 따른 의견서(한 개 이상의 회원국에서 적용되는 문제에 대한 EDPB의 의견서)를 6개 채택하였는 바, EDPB의 의견이 GDPR의 일관된 해석에 도움이 되어 왔다고 평가하였다. 그러나 시민단체인 엑세스 나우는 원스탑샵 시스템이 국경간 분쟁을 효과적으로 해결하고 기관간 협력을 요하는 사건을 원활히 처리할 수 있을지 의문을 제기하며 특정 국가 감독기관보다 EDPB의 역할이 핵심적이라고 지적하였다. 감독기관의 자원 측면에서는 전반적으로 인적, 재정적으로 부족한 상태이며, 회원국 간에도 불균등하다는 것이 집행위원회, EDPB, 엑세스 나우 등의 공통된 평가이다.

특히 엑세스 나우는 감독기관이 자원이 부족할 경우, 법 집행이 안되고 법이 무시되는 상황이 벌어질 수 있다고 경고하며, 자원이 풍부한 거대 기술기업과 소송이 벌어졌을 때 장기간의 소송 보다 기업에 유리한 합의를 할 가능성을 우려하였다.

셋째, 개인정보 규범의 조화 측면에서 보았을 때, 유럽연합 역내에서 통일적인 단일 규범을 적용하려는 GDPR 주요 제정 목적에도 불구하고 정보사회 서비스에 동의할 수 있는 아동의 연령 등 일정한 분절(fragmentation)이 여전히 남아있다. 또 하나의 문제는 개인정보 보호와 표현의 자유 사이의 조화 문제로서, 엑세스 나우도 많은 공공기관들이 언론의 자유나 시민사회 활동을 제약하기 위해 GDPR을 남용하고 있다고 비판하였다. 한편, 집행위원회와 EDPB는 건강 및 연구 목적의 민감정보 처리 금지 예외의 경우나 과학적 연구를 위한 개인정보 처리와 관련한 통일된 규범 수립을 위해 노력하고 있다.

넷째, 정보주체의 자기정보 통제권의 강화 측면에서 집행위원회는 개인들이 자신의 권리를 점차 인지해가고 있으며, GDPR은 절차적인 권리도 강화했는데 대표소송에 관한 디렉티브(Directive on representative actions)가 채택되면 각 회원국에서 집단 소송을 활성화하고 국경간 소송 비용을 낮출 수 있을 것으로 전망했다. 또한 개인정보 이동권의 잠재력을 발전시키는 것이 집행위원회의 우선순위가 될 것이라고 한다.

다섯째, GDPR의 적용이 특히 중소기업에게 위협이 된다는 지적에 대하여 집행위원회는 기업 규모에 따라 예외를 적용하는 것은 부적절하다고 보았다. 다만, 감독기관들이 개인정보 침해 위험이 적은 중소기업들의 GDPR 이용을 도울 수 있다.

여섯째, GDPR의 원칙을 인공지능, 블록체인, 사물인터넷, 얼굴인식 등 특정 기술에 어떻게 적용할지 명확히 할 필요가 있고 계속적인 모니터링이 필요하다.

일곱째, GDPR은 개인정보의 국제적인 이전을 위하여 적정성 결정 등 여러가지 도구들을 제공하고 있다. 유럽연합은 2019년 2월 일본과 적정성 결정을 체결하였으며, 한국과는 진전된 단계(advanced stae)이며 아시아 및 남미 국가들과 모색을 위한 대화(exploratory talk)를 진행 중이다. EDPB는 일본의 사례와 같은 추가적인 규칙에 의존하는 적정성 구조가 지속가능하고 신뢰할 수 있는 시스템인지 보장할 필요가 있다고 촉구하였다.

여덟째, 개인정보 분야의 수렴(convergence) 및 국제 협력의 증진 측면에서, 집행위원회는 GDPR을 모델로 하여 전 세계의 개인정보 보호 법제가 수렴되는 현상을 바람직한

것으로 평가하며, 그러한 방향에서 글로벌한 대화를 강화하겠다고 밝혔다. 다만 EDPB는 집행위원회가 국제 무역협상에서 데이터의 자유로운 흐름에 대한 논의 이전에 GDPR이나 적정성 결정에 따른 강력한 개인정보 보호를 제공할 필요가 있다고 지적하였다.

라. 유럽사법재판소의 개인정보 관련 주요 결정

2015년 유럽사법재판소는 세이프하버 협정을 무효라고 판결하였다(이른바 '슈렘스 I 판결'). 세이프하버 협정을 수립한 EC 결정 2000/520은 미국이 자국 법이나 국제조약을 통해 사실상 동등한 보호수준을 보장할 것을 언급하지 않았으며 따라서 세이프하버 원칙의 내용을 살펴볼 것도 없이, EC 결정 2000/520의 1조가 개인정보보호지침 25(6)조에서 명시한 요구조건을 준수하지 못했으므로 무효이다. 더불어 EC 결정 2000/520의 3(1)조는 국가 감독기관의 권한을 규정하고 있는데, 국가 감독기관이 매우 제한적인 조건에서만 개입할 수 있도록 하고 있다. 이는 국가 감독기관의 권한을 부인하는 것으로 3(1)조의 채택은 집행위원회의 권한을 넘어서는 것으로서 무효이다. 유럽사법재판소는 제3국의 개인정보 보호 수준이 실질적으로 유럽연합의 보호수준과 동등해야 한다고 보고 있으며, 정보수사기관 등이 개인정보에 접근할 때에도 필요성과 비례성의 원칙을 준수하고 정보주체에게 적절한 구제수단을 제공해야 함을 중요하게 판단하고 있다는 점, 그리고 집행위원회에 의해 적정성 결정이 체결되더라도 향후에 개별 국가의 감독기구에 의해 다른 판단이 내려질 수도 있다는 점은 현재 유럽연합과 적정성 결정을 추진하고 있는 한국의 입장에서도 심각하게 고려해야할 내용이다.

유럽사법재판소 판결 이후, EU 집행위원회와 미국 정부는 세이프하버 협정을 대체할 새로운 체제를 협의하였고, 2016년 7월 12일 프라이버시 쉴드 협정을 체결하였다(2016/1250 결정). 유럽사법재판소는 2020년 7월 16일 내린 C-311/18 판결에서, 프라이버시 쉴드 협정 역시 미국의 국가안보, 공익, 법집행 요구 조건을 우선시 하여 미국으로 이전된 개인정보 주체의 기본권이 침해되고 있다고 보고 무효로 판결하였다(이른바 '슈렘스 II 판결'). 유럽사법재판소는 국가안보를 목적으로 미 당국의 개인정보 접근을 가능하게 하는 법률의 제도적 보호조치 및 정보 접근과 관련하여 정보주체에게 명확한 정보제공 등의 권리 보장이 필요한데, 미 당국의 정보접근 및 감시 프로그램을 감독하는 옴부즈만 제도가 GDPR 58(2)조에 비례한 독립성을 보장하고 있지 못하며, 미 당국을 대상

으로 유럽연합의 정보주체가 제기할 수 있는 권리 이행 방안이나 법적 구제 방안이 미흡하다고 판결하였다.

2016년 10월 19일, 유럽사법재판소는 C-582/14 판결에서 IP주소, 특히 인터넷에 연결할 때마다 매번 변화하는 유동 IP 주소가 개인정보라고 판결하였다. 유럽사법재판소는 어떤 정보가 개인정보가 되기 위해서 "정보주체의 식별을 위한 모든 정보가 한 사람의 손에 있어야 하는 것은 아니"라며, ISP에서 이용자를 식별할 수 있는 추가정보를 보유하고 있는 한 유동 IP주소의 이용자는 형사절차 과정 등에서 식별될 수 있다는 것이다.

2014년 5월 13일, 유럽사법재판소는 C-131/12 판결에서 구글이 검색 결과 목록에서 한 이용자의 경제적 어려움에 대한 오래된 정보를 삭제할 의무가 있는지에 대한 판결에서 그러한 의무를 인정하였다(이른바 '잊힐 권리 판결'). 이 판결에서 유럽사법재판소는 구글이 정보를 찾아 웹을 검색(크롤링)하고 검색 결과 제공을 위해 콘텐츠를 인덱싱할 때, 유럽연합 법 하에서 책임과 의무를 가진 컨트롤러가 된다고 보았다. 다음으로 검색엔진 운영자의 활동도 개인정보의 '처리'라고 보았다. 유럽사법재판소는 인터넷 검색 엔진 및 개인정보를 제공하는 검색 결과가 개인에 대한 상세한 프로파일을 구축한다고 보았으며, 그 개인정보 처리가 더 이상 필요하지 않거나 시기가 지난 것(outdated)일 때 검색엔진에도 정보주체의 삭제권이 적용된다.

잊힐 권리에 대한 유럽사법재판소의 판결은 개인정보 보호와 표현의 자유를 둘러싼 전 세계적인 논란을 촉발시켰다. 유럽사법재판소는 2019년 잊힐 권리와 관련된 후속 판결 두 개로 이 문제에 대한 좀더 진전된 기준을 제시하였다. 2019년 9월 24일 C-136/17 판결에서 유럽사법재판소는 구글 스페인 판결에서와 마찬가지로, 검색 엔진 역시 컨트롤러로서 민감 정보의 처리에 대해 책임을 진다고 보았다. 그런데 검색 엔진은 정보주체의 기본권과 일반 대중의 정보 자유의 균형을 맞추어야 한다. 이때 문제가 되는 정보의 성격이나 정보주체의 사생활에 미치는 민감성과 정보에 접근할 일반 대중의 이익을 고려해야 하는데, 이는 공적 영역에서 정보주체의 지위에 따라 달라질 것이다. 또 C-507/17 판결에서는 잊힐 권리가 모든 유럽의 도메인 영역에 적용된다고 판결하였다.

특히 유럽사법재판소는 여러 판결을 통해 개인정보 감독기관의 '완전한 독립성'의 의미를 구체화하였다. 특히 독일 개인정보 감독기관에 대한 C-518/07 판결에서 개인정보 감독기관들이 지침에서 보장된 개인정보 처리와 관련된 권리의 '수호자'이며, 완전히

독립적인 감독기관의 설치는 “개인정보의 처리와 관련하여 개인을 보호하기 위한 필수적인 구성요소”라고 강조하였다. 개인정보 감독기관이 ‘완전한 독립성’을 가지고 기능하는 것에 대한 법적 요건은 피감독 기관들로부터의 영향만이 아니라 국가나 주의 직접 또는 간접적인 영향을 포함하여, 어떠한 외부의 영향력으로부터도 자유로운 의사결정 권한을 의미한다. C-614/10 판결에서는 오스트리아의 개인정보 보호 감독기관의 상임위원 및 사무처의 직제에 있어서 완전히 독립적이지 않다고 보았고, C-288/12 판결에서는 헝가리의 개인정보 보호 감독기관의 재직기간이 전 임기를 보장하고 있지 않다는 점에서 완전히 독립적이지 않다고 보았다.

2. 미국

미국은 유럽연합 등 다른 나라에 비해 상대적으로 빅데이터의 활용에 유리한 법적 환경을 가지고 있는 것으로 통상적으로 평가받고 있지만, 2010년 3월 미 연방거래위원회(FTC)는 인터넷 사용자들의 프라이버시 보호를 위해 <급속한 변화의 시대의 소비자 개인정보 보호> 보고서를 발간하는 등 오바마 정부 하에서 미국 역시 빅데이터 등 변화하는 정보통신환경에 대응하여 개인정보 보호를 강화하는 움직임을 보여 왔다. 이러한 오바마 행정부의 개인정보 보호 강화 정책은 트럼프 행정부 내에서 이어지지 못했다.

2018년 6월 28일 캘리포니아 주에서 ‘캘리포니아주 소비자 프라이버시 보호법(The California Consumer Privacy Act of 2018, CCPA)’이 채택되었다. CCPA는 GDPR과 흡사하게 개인정보 보호에 대한 광범위한 내용을 규정하고 있으며, 캘리포니아 주에서 사업을 하는 일정 조건의 영리 기업에게만 적용된다는 한계가 있지만 소비자 프라이버시 보호라는 관점에서 제정된 개인정보 보호법제라는 점, 주민의 제안에서 발의가 시작되었다는 점에서 큰 의의를 지닌다.

CCPA 통과 이후, 네바다 주의 ’인터넷 프라이버시법’ 등 다수의 다른 주에서도 포괄적인 개인정보 보호법이 제안되었으며, 연방 차원에서도 포괄적인 프라이버시법이 제안되고 있다.

3. 일본

일본의 개인정보 보호법은 2003년 5월에 제정된 후, 기술 환경의 변화에 대응하가 위해 2015년에 개정되었다. 개정 개인정보 보호법은 개인정보의 정의 명확화, 익명가공정보 개념 도입, 요(要)배려 개인정보 보호 강화, 추적가능성 조항, 명부업자에 대한 규제 강화, 개인정보 감독기관으로서 개인정보 보호위원회 설립 등의 내용을 담고 있다.

한편, 2019년 1월 23일 일본 개인정보 보호위원회와 유럽집행위원회는 양국의 개인정보 보호체계가 동등한 수준이라고 인정하는 상호 적정성 평가를 최종적으로 승인하였다. 이를 위해 일본 정부는 유럽연합에서 이전되는 개인정보에 대해서만 적용되는 보조규칙을 마련했다. 이는 일본의 개정 개인정보 보호법이 GDPR에 비추어 미흡한 부분이 있었기 때문인데, 보조규칙을 통해 GDPR과 동등한 수준을 확보하고자 한 것이다. 우리나라도 현재 유럽연합의 적정성 결정을 추진 중인데, 추가적인 보조규칙을 두기 보다는 GDPR 수준으로 개인정보 보호법을 개정하는 것이 바람직하다.

제3장 국내 개인정보 보호법제의 현황과 쟁점

제1절 신기술과 개인정보를 둘러싼 사회적 논란의 경과

빅데이터 분석 목적의 개인정보 활용에 대한 논란은 결국 '비식별 처리된 정보', 즉 '가명정보' 활용의 적법성 논란이라고 볼 수 있다. 정부는 개인정보의 수집 목적 외 활용을 위해 가이드라인에 '비식별'이라는 법적 근거가 없는 개념을 도입해 가명정보를 일정한 조건 하에 활용할 수 있도록 했고, 이는 자연스럽게 개인정보 보호법 위반 논란을 야기했다. 법에 근거하지 않은 개념을 사용했을 뿐 아니라, 가이드라인에 따라 비식별에 대한 개념도 바뀌어 수범자의 혼란을 가중시켰다. 비식별(de-identification)이란 개인정보에서 식별자를 제거하는 것을 의미하는데 식별자를 어떻게, 얼마나 제거하느냐에 따라 그 결과는 다른 정보와 결합해도 더 이상 개인을 식별할 수 없는 익명정보(anonymised data)가 될 수도 있고, 다른 정보와 결합하면 개인을 식별할 수 있는 가명정보(pseudonymised data)가 될 수도 있다.

2016년 박근혜 정부는 정부 부처 합동으로 〈개인정보 비식별조치 가이드라인〉을 발

표하였다. 그러나 비식별 조치의 개념은 개인정보 보호법에 근거가 없을 뿐만 아니라, 비식별 처리된 정보로 인한 개인정보 침해가 발생할 경우 법적 책임을 누가 질 것인지 모호하게 규정하고 있다. 특히 결합에 사용되는 정보집합물의 경우 임시대체키를 사용하기 때문에 익명정보로 보기에는 무리가 있는데, 따라서 전문기관을 통한 정보집합물의 결합은 정보주체의 동의없는 제3자 제공으로서 개인정보 보호법 위반 소지가 있었다. 이에 시민사회단체들은 2017년 국정감사를 통해 3억 4천여 만 건의 사용자 개인정보가 동의 없이 결합되어 기업에 제공된 것이 드러나자, 비식별 전문기관과 20개 기업을 개인정보 보호법 등 위반으로 검찰에 고발하였다.

문재인 정부 역시 빅데이터 환경에서 개인정보 활용을 모색하려는 취지로 대통령 산하 4차산업혁명위원회에서 '규제·제도혁신 해커톤'을 운영하였다. 2차·3차 해커톤에서는 비식별화라는 용어보다는 '개인정보, 가명정보, 익명정보'로 개인정보와 관련된 법적 개념체계를 정비하기로 합의하였으나 가명정보의 활용 목적과 범위에서 완전한 합의에 이르지 못하였다. 해커톤에서의 논의 이후 정부는 개인정보 보호 법제의 개정을 추진했는데, 정부가 '개인정보의 활용'에 초점을 두었다면 시민사회단체는 개인정보 보호법제의 정비와 감독기구의 통합을 촉구했다. 정부의 데이터 정책은 2018년 11월, 개인정보 보호법, 신용정보법, 정보통신망법 등 3개 법안의 개정안으로 구체화되어 발의되었다. 정부는 이를 '데이터 3법'이라고 홍보했으나 시민사회단체들은 '개인정보 도둑법'이라 비판하였다. 데이터 3법은 시민사회의 반대와 국회 논의 과정에서의 논란에도 불구하고, 결국 2020년 1월 9일 국회를 통과하였다.

제2절 데이터 3법의 주요 쟁점 및 문제점

1. 개인정보 보호 체계의 개선과 한계

그동안 한국의 개인정보 보호체계의 문제점으로 연구자들과 시민사회에서 일관되게 지적해온 문제는 다원적인 개인정보 보호 법제와 독립적인 감독기구의 부재였다. 2016년 10월, 한국 정부가 추진해온 GDPR 적정성 평가가 개인정보 감독기구의 독립성과 권한 미비 문제로 EU 집행위원회로부터 부적격 통지를 받았고, 이후 방송통신위원회가 추진해 온 '부분 적정성 평가'도 원활히 이루어지지 못했다. 그러자 정부는 데이터3법에서 개

인정보 보호 법제 및 감독체제를 정비하기로 하였고 2020년 1월 데이터 3법 통과로 개인정보 보호 법제의 통합과 독립적인 감독기구의 설립이 일부 이루어졌다. 그러나 보호법제와 감독기구의 일원화라는 관점에서는 미흡한 점이 남아 있다.

첫째, 신용정보법의 개인정보 관련 조항은 여전히 그대로 남아있으며 금융위원회 역시 개인신용정보에 대한 감독권한을 유지하고 있다. 둘째, 개인정보 보호법과 신용정보법의 유사·중복 규정으로 인한 혼란이 여전히 남아있으며, 오히려 심화된 측면도 있다. 예를 들어, 개인정보의 정의에서부터 유사하지만 차이가 있으며, 개인정보 보호법에는 익명처리의 개념이 없지만 신용정보법에서는 두고 있다. 개인정보 보호법에서는 '과학적 연구'라는 개념을 사용하고 정의 규정을 두고 있지만, 신용정보법은 정의 규정 없이 '연구'라는 개념을 사용하고 있다. 셋째, 정보통신망법의 개인정보 관련 조항을 개인정보 보호법으로 흡수한 것은 바람직한 방향이지만, '특례' 형식으로 포함되었기 때문에 여전히 정보통신서비스 제공자인지 여부에 따라 별도의 취급을 받게 되었다. 넷째, 새로 출범한 개인정보 보호위원회의 독립성에 대해서도 우려가 제기되고 있다. 개인정보 보호와 관련된 법령의 개선이나 개인정보 보호와 관련된 정책에 있어서 여전히 국무총리의 지휘·감독을 받고 있기 때문에 개인정보 감독기관으로서 전문성이 아니라 정부의 정치적 지향에 영향을 받을 우려가 있다.

2. 개정 개인정보 보호법을 둘러싼 쟁점

가. 개인정보의 개념

GDPR(전문 26)이 개인정보 식별의 주체를 '컨트롤러나 다른 사람(by the controller or by another person)'로 보고 있는 것과 달리, 정부는 2016년 <개인정보 비식별조치 가이드라인> 안내서에서부터 2020년 <가명정보 처리 가이드라인>에 이르기까지 '알아볼 수 있는'의 의미를 "해당 정보를 '처리하는 자'의 입장에서" 판단해야 한다고 폭좁게 해석하고 있다. 즉, 해당 정보를 '처리하는 자'의 입장에서 알아볼 수 없다면 개인정보가 아니라는 것인데 개인정보성을 부정하는 것은 아예 개인정보 보호법 자체를 배제하게 되기 때문에 위험하다. 반면 법원은 '쉽게 결합하여'의 의미를 "쉽게 다른 정보를 구하기 쉬운지 어려운지와는 상관없이 해당 정보와 다른 정보가 특별한 어려움

없이 쉽게 결합하여 특정 개인을 알아볼 수 있게 되는 것을 말한다" 고 판시하고 IMEI와 USIM 일련번호 역시 개인정보라고 보았다는 점에서 정부의 해석과 차이가 있다. 유럽사법재판소도 유동 IP 주소가 개인정보인지 여부에 대한 판결에서 유사한 해석을 내린 바 있다.

나. 가명처리와 가명정보의 의의

개인정보 보호법의 개념 체계를 GDPR로부터 차용했음에도 불구하고, '가명처리' 개념이 활용되는 맥락은 GDPR과 차이가 있다. GDPR은 가명정보를 정의하고 있지 않으며, 유럽기본권청이 발간한 <유럽의 개인정보 보호 법률 핸드북>에서는 유럽의 법률에는 '가명정보(pseudonymised data)' 라는 개념이 없다고 설명한다. 즉, 유럽에서는 가명정보라는 특정한 상태나 그 방법이 정해져있는 것이 아니라, 개인정보 침해 위험을 줄이기 위한 암호처리 등 여러 '안전조치' 의 하나로서 가명처리를 인식하고 있으며 다양한 방식과 수준의 가명처리가 가능하다고 보고 있다. 반면 개정 개인정보 보호법에서는 가명정보의 개념을 정의하여 마치 특정한 가명정보가 존재하는 것처럼 오해할 수 있을 뿐만 아니라, 서로 다른 개념인 가명처리와 가명정보의 처리를 같은 것으로 다룸으로써 관련된 여러 규정에 혼란을 야기하고 있다. 예를 들어, 제28조의7은 가명정보에 대해 정보주체의 열람권을 배제하고 있는데 가명처리에 대해서도 열람권을 배제하는 것인지가 문제가 될 수 있다. 또 GDPR에서는 개인정보를 목적 외로 활용하든 그렇지 않든, 개인정보의 가명처리가 가능하다면 안전조치의 하나로서 하는 것이 좋다고 보고 있는 데 반해, 개정 개인정보 보호법은 당초 수집 목적 외 처리를 위한 조건으로 가명처리를 인식하고 있다. 즉, 마치 가명처리만 하면 정보주체의 동의 없이 과학적 연구 목적으로 사용할 수 있는 것처럼 규정하고 있으며, 그 자체로 원래의 개인정보를 보유하고 있는 개인정보처리자 뿐만 아니라 가명정보를 제공받는 제3자 개인정보처리자 역시 별도의 적법성 요건을 갖출 필요 없이 과학적 연구 목적으로 활용할 수 있도록 하고 있다.

다. 과학적 연구의 범위

개인정보 보호법 개정 과정에서 가장 논란이 되었던 이슈 중 하나가 과학적 연구의

범위였다. 시민사회는 빅데이터나 인공지능 기술의 개발에 반대하는 것은 아니지만, 정보주체의 동의 없는 개인정보의 목적 외 활용은 '학술연구'로 제한되어야 한다고 본다. "누군가 자신의 행위를 '연구'라고 지칭한다고 무조건 허용하는 것이 아니라, 과학적 방법을 사용하고 과학적 가치가 있는 것이어야" 하며, "연구 결과물의 공개 등을 통한 과학적, 기술적 기반 확대라는 사회적인 기여가 인정되어야" 한다는 것이다. 왜냐하면, "학술 연구나 통계작성을 위해 일정하게 정보주체의 권리를 제약하는 것은 그에 상응하는 사회적인 가치와 기여가 있기 때문"이며, 순전히 사적인 이익을 위한 개인정보 활용을 위해 정보주체의 권리를 제한해야 할 이유가 없다는 것이다. GDPR은 과학적 연구(scientific research)에 대한 정의를 별도로 두고 있지 않다. 다만, EDPS는 과학적 연구의 개념을 검토하면서 "개인정보처리자가 단지 과학적 연구 목적이라고 주장하는 것으로는 충분하지 않"으며, "과학적 연구가 전체 사회에 유용하며 과학적 지식이 촉진되고 지원해야 할 공공재라는 점을 공통된 전제로 한다"고 보고 있다. 또한 과학적 연구를 위한 개인정보 보호체계의 하나의 기준으로 연구가 주로 사적인 이익이 아니라 사회 전체적인 지식 및 복리의 향상을 목적으로 수행될 것 등을 제시하고 있다.

라. 가명정보의 결합

2016년 〈개인정보 비식별조치 가이드라인〉 당시부터 큰 논란의 대상이 되었던 이슈 중 하나가 개인정보의 결합이었다. 개정 개인정보 보호법에서는 일정한 요건을 갖추면 개인정보 보호위원회나 관계 중앙행정기관의 장이 민간업체도 전문기관으로 지정할 수 있도록 하였고, 시행령에서 한국인터넷진흥원을 결합키 관리기관으로 지정하여, 결합키를 생성하는 결합키 관리기관과 결합을 수행하는 전문기관의 역할을 구분하였다. 문제는 결합된 가명정보를 원 개인정보처리자가 반출할 수 있도록 허용한 것이다. 이에 시민사회단체들은 가명정보 결합에 대해 "기업들에게 고객정보를 판매하고 공유할 수 있도록 하는 것"에 다름 아니라고 비판한다. 비록 가명처리를 하더라도 결합된 개인정보는 재식별의 위험성이 높아질뿐더러, 나아가 원래의 개인정보 데이터베이스를 보유하고 있는 개인정보처리자에게는 최소한 기술적으로는 재식별이 쉽게 가능할 수 있기 때문이다. 국가인권위원회는 개인정보 보호법 시행령 일부개정령안에 대한 검토서에서 "가명 결합정보의 구체적 반출요건을 전면 재검토하고, 고시가 아닌 시행령에 구체적으로 규정할 것"과

외부 반출된 결합가명정보가 금전적 대가를 받고 판매·거래되는 행위를 금지하는 명시적 규정을 보완할 것을 권고하였지만 수용되지 않았다.

마. 정보주체의 권리 제한

개정 개인정보 보호법 제28조의7은 가명정보에 대해 정보주체의 권리와 관련된 다수 규정의 적용을 배제하고 있다. 가명정보를 처리하더라도 항상 정보주체의 권리 보장이 불가능하거나 혹은 그 권리를 보장하는 것이 정보주체에게 해를 미치게 되는 것은 아님에도 정보주체의 권리에 해당하는 모든 조항을 무조건 적용 배제하는 방식은 타당하지 않다. GDPR의 경우 제89조의 2항에서 개인정보가 과학적 또는 역사적 연구 목적이나 통계적 목적으로 처리되는 경우 정보주체의 권리를 일부 제한할 수는 있지만, 무조건 해당 조항의 적용을 배제하는 것이 아니라 "정보주체의 권리를 보장하는 것이 특정한 처리 목적의 달성을 불가능하게 하거나 중대하게 손상시킬 것으로 예상되고, 처리 목적을 달성하기 위하여 권리 적용을 일부 제외할 필요"가 있을 때에 한한다. 특히 개인정보 파기에 대한 제21조의 배제가 특정 목적에 대한 규정 없이 가명정보를 무기한 보관하는 것을 의미한다면 이는 개인정보 보호를 위한 국제규범이나 개인정보 보호법 제3조의 보호원칙에 위반된다.

바. 과학적 연구 목적의 민감정보 활용

개정 개인정보 보호법의 '제3절 가명정보의 처리에 관한 특례'가 제23조 민감정보에도 적용되는지에 대해서 논란이 있을 수 있다. 특히 의료정보를 포함한 개인 건강정보는 개인의 권리에 치명적인 영향을 미칠 수 있는 민감정보이지만, 보건의료 분야의 연구 등 공공적, 산업적 측면에서 활용 가치가 높은 정보로 인식되고 있다. 가명정보 역시 개인정보이기 때문에 제23조에 따라 정보주체의 별도 동의나 법령의 근거 없이는 제3절 가명정보의 처리에 관한 특례에 따라 처리할 수 없다고 볼 수 있다. 그러나 2020년 9월 보건복지부와 개인정보 보호위원회가 공동으로 발간한 <보건의료 데이터 활용 가이드라인>에서는 제3절의 규정이 민감정보에도 적용된다고 해석하고 있다. 국내 개인정보 보호법은 과학적 연구 목적 처리에 있어서 일반적인 정보와 민감정보의 구분이 없는 것처럼 해석한 것이다. 이는 민감정보의 처리를 원칙적으로 금지하고 특별히 보호하고자 한 취

지를 무시한 것이다. GDPR의 경우 과학적 연구 등의 목적을 위해 민감정보의 처리를 허용하되 정보주체의 권리 침해를 방지할 수 있는 충분한 안전조치를 규정하는 별도의 법률에 근거하도록 하였다.

사. 개인정보의 추가적인 이용·제공 기준

개정 개인정보 보호법 제15조 3항 및 제17조 4항은 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용하거나 제공할 수 있도록 규정하였다. 이 규정은 수집 목적과 다른 목적으로 추가 처리될 가능성을 배제하지 않는다는 점에서 처음부터 권리 침해의 가능성을 내포하고 있다. 이 규정은 GDPR의 제6조 제4항의 규정을 국내에 도입한 것이다. 이 규정이 정보주체의 합리적 기대를 벗어나는 방식으로 추가 처리하는 것을 합리화하지 않도록 주의할 필요가 있다.

3. 신용정보법을 둘러싼 쟁점

신용정보법에 대해서도 개인정보 보호법에서처럼 가명처리한 개인신용정보의 연구 목적 활용 및 연계와 관련한 논란이 제기된다. 신용정보법에 대해 고유하게 제기된 문제는 다음과 같다.

가. 개인신용정보의 범위

최근 개인신용정보의 개념에 쇼핑몰 거래 내역을 포함하는 문제가 불거진 것은 개인신용정보의 정의가 개정된 데 따른 것이다. 개인신용정보를 금융거래와 관련된 상거래로 한정하여 규정하였던 전과 달리 “상행위에 따른 상거래의 종류, 기간, 내용, 조건 등에 관한 정보“를 폭넓게 포함한 데 따른 논란이 계속되고 있다. 이는 개인정보에 대한 감독권한이 개인정보 보호위원회와 금융위원회로 이원화된 상황이 초래한 혼란과 갈등으로 볼 수 있다. 이러한 혼란을 해소하기 위해 신용정보법은 금융 및 신용정보 산업에 대한 규율을 다루고 개인정보와 관련된 규율은 개인정보 보호법으로 일원화할 필요가 있다.

나. 익명처리에 대한 적정성 평가

신용정보법은 익명처리에 대한 적정성 평가에서, 적정성 평가가 제대로 되지 않았을 경우 그 책임에 대하여 명확히 규정하지 않았다. 익명처리가 된 것으로 생각했으나 제대로 익명처리가 되지 않아 정보주체에게 피해가 발생할 경우, 개인정보처리자가 어떻게 책임을 질 것인지, 적정성 평가를 잘못하여 피해를 야기한 금융위원회 및 데이터전문기관이 어떠한 책임을 지는 것인지 명확하지 않다. 아무런 책임도 없다면 산업 활성화를 명분으로 손쉽게 적정성 평가를 남발할 가능성을 배제할 수 없다.

다. 공개된 SNS 정보의 수집과 표현의 자유 침해 우려

개정 신용정보법은 "신용정보주체가 스스로 사회관계망서비스 등에 직접 또는 제3자를 통하여 공개한 정보"에 대하여 신용정보주체의 동의를 받지 않아도 되는 예외로 규정하였던 당초 개정안에 대하여 논란이 일자 "이 경우 대통령령으로 정하는 바에 따라 해당 신용정보주체의 동의가 있었다고 객관적으로 인정되는 범위 내로 한정한다"는 단서를 추가하였다. 그러나 국가인권위원회가 의견을 표명한 바와 같이, 정보 주체가 SNS에 스스로 공개한 개인정보라고 하더라도 신용정보 회사가 아무런 제약 없이 수집·이용할 수 있다고 보기는 어려우며, 이용자들이 신용평가를 우려하여 SNS 사용이 위축되고 표현의 자유가 침해될 우려가 있다.

라. 개인신용정보 전송요구권과 마이데이터 사업

개정 신용정보법은 '개인신용정보 전송요구권'을 신설하여 마이데이터 사업자가 보다 효율적으로 개인정보를 수집할 수 있는 수단을 제공하고 있다. 그러나 전송요구권이 GDPR 제20조 개인정보 이동권을 국내에 도입한 것이라는 금융위원회의 주장과 달리 마이데이터가 서로 다른 사업자들이 보유하고 있는 개인정보의 통합을 지향하고 사업자 편의를 위해 개인신용정보 활용을 촉진하고자 한다는 점에서 이용자가 한 서비스 제공자로부터 다른 서비스 제공자로 전환하는 모델을 상정하고 있는 GDPR의 이동권과 다른 개념이다. 사업자의 편의를 위한 마이데이터 사업은 정보주체의 통제권을 강화하기 보다는 개인정보의 유통이나 활용을 강화할 우려가 있다.

마. 법체계 문제 - 하위 규범으로의 지나친 위임

신용정보법이 지나치게 많은 내용들을 하위 법령에 위임하고 있는 점도 문제로 지적된다. 또한 법률에서 시행령에 위임한 사항을 더 구체화하지 않고 고시로 재위임하고 있는 조항도 다수 발견된다. 신용정보법에서 대통령령으로 위임하고 있는 사항이 무려 약 250여 개에 이른다고 한다. 특히 '신용정보'의 개념과 관련하여 무려 17부분을 대통령령에 위임하였다.

제3절 국내 개인정보 보호법제 개선 방향

조만간 개인정보 보호법의 개정이 불가피하다. 지금까지의 분석을 토대로 국내 개인정보 보호 법제의 개선 방향을 제시하자면 다음과 같다.

첫째, 우선 개인정보 보호 법제에 여전히 남아있는 모호함을 해소하는 방향으로의 정비가 필요하다. 정보통신망법과의 실질적인 통합, 가명정보 특례의 모호한 규정의 명확화, 민감정보의 과학적 연구 목적의 처리 등이다. 둘째, 개인정보 보호법과 신용정보법, 그리고 위치정보법 등 개인정보 보호 법제를 일원화하는 방향으로 추가 정비할 필요가 있다. 셋째, 빅데이터, 인공지능 등 신기술 환경에서 정보주체의 권리를 보호하고 개인정보처리자의 책임성을 강화하기 위한 새로운 규범들을 도입할 필요가 있다. 프로파일링 등 자동화된 개별 의사결정에 대한 정보주체의 권리 등의 권리를 도입하고, 개인정보 영향평가, 설계 및 기본설정에 의한 개인정보 보호 등 책임성 강화 제도의 도입도 필요하다. 넷째, 국내 개인정보 보호법의 경우 정보수사기관의 개인정보 처리에 대해서는 폭넓은 예외를 허용하고 있는 만큼, 국제적인 기준에 맞게 규범을 재정비하고 이들 기관에 대한 감독을 강화할 수 있는 방안을 모색해야 한다.

제4장 정보주체의 권리보호

제1절 정보주체의 권리보호를 위한 개인정보 처리원칙

우리나라의 개인정보 보호법상 개인정보 보호 원칙은 국제규범인 GDPR의 적법성·공

정성·투명성 원칙에 입각하고 있다고 볼 수 있다. 하지만 원칙 규정에 있어서도, 개인정보 보호를 위한 가장 필요한 규범적 원칙은 GDPR의 규정에서 보는 것처럼 구체적으로 정할 필요가 있다. 특히 개인정보 처리의 목적 제한의 원칙, 데이터 최소화 원칙, 정확성 원칙, 보관기간 제한 원칙, 무결성과 기밀성 원칙에 대한 보다 자세한 내용을 규정하고, 적절한 기술적, 조직적 조치를 활용한 무단 또는 불법 처리 등으로부터 개인정보의 적절한 보안을 보장하는 방식으로 개인정보처리자가 처리할 것 등 보호조치 강화와 그 책임이 강조되어야 한다. 또한 개인정보 수집 및 보유 사유 등에 대한 명확한 증명책임, 개인정보 처리원칙의 준수책임과 그에 대한 증명책임을 개인정보처리자 등(개인정보의 처리 등에 대한 규범 준수자)에게 지우는 원칙이 필요하다.

제2절 정보주체의 개인정보 처리 정보를 제공받을 권리, 접근권, 수정권, 삭제권, 처리 제한권

우리나라 개인정보 보호법의 정보주체의 권리는 대체로 GDPR의 정보주체의 권리와 유사하며, CCPA와 일본 개인정보 보호법의 정보주체의 권리의 내용도 포함하고 있는 것으로 볼 수 있다. 하지만 정보주체의 권리행사를 보장하기 위한 구체적인 방법에 있어 차이가 있다.

가장 큰 문제는 실제에 있어 우리나라 개인정보 보호법에 규정된 정보주체의 권리는 그 행사가 거의 이루어지고 있지 않다는 점이다. 그 이유는 정보주체가 자신이 행사할 수 있는 권리가 무엇이며, 그 내용은 무엇인지를 제대로 인식하지 못하고 있는 것이 가장 큰 요인으로 생각된다. 이것은 정보주체의 권리행사를 보장하고 실행할 수 있도록 하기 위한 법규범이 미흡한 점에서부터 비롯한다. 이에 대한 개선을 위해, 특히 GDPR의 정보주체의 권리행사를 위한 투명한 정보, 통지 및 형식에 대한 규정을 참조하여 우리법에도 규정함으로써 개인정보 처리 정보를 제공받을 권리를 실효성 있게 강화할 필요가 있다. 우리나라 개인정보 보호법은 정보주체의 동의를 받을 때에만, '알아보기 쉽게 표현'하라고 규정되어 있을 뿐이다. 따라서 동의에서부터 처리에 이르기까지, 정보주체에게 자신의 권리 및 행사 방법을 고지하고, 정확하고 투명하며 이해하기 쉬운 형식으로 명확하고 평이한 언어를 사용하여 제공할 것을 명확히 규정할 필요가 있다. 열람, 정정,

삭제권 등 정보주체가 행사할 수 있는 권리의 존재 및 권리행사 방법, 향후 동의를 철회할 수 있는 권리, 감독기관에 민원을 제기할 수 있는 권리, 처리의 법적 근거, 개인정보를 제공할 의무가 있는지 여부, 위탁할 경우 위탁자 및 위탁의 내용(현재 개인정보처리방침에만 공개하도록 하고 있음) 등 정보주체의 권리행사 등을 위해 필요한 항목에 대한 내용 측면에서의 개선이 필요하다.

우리나라 개인정보 보호법은 개인정보의 처리 여부를 확인하고 개인정보에 대하여 사본의 발급을 포함한 열람을 요구할 권리를 보장하며(제4조), 구체적으로는 처리하는 자신의 개인정보에 대한 열람을 보장한다(제35조). 하지만, '개인정보의 처리 여부 및 처리의 방법'이 열람권의 대상으로 제35조에 명시되어 있지 않다는 점은 문제이다. 따라서 이 경우에도 정보주체 자신의 개인정보의 처리 및 처리자가 보유하고 있는 개인정보, 정보주체의 권리 및 행사 방법 등 모든 관련 정보를 열람할 수 있도록 개선해야만 한다. 또한 열람권 행사를 위해서는 개인정보처리자가 서면, 전화, 전자우편, 인터넷 등 정보주체가 쉽게 활용할 수 있는 방법으로 제공하며 인터넷 홈페이지에 열람 요구 방법과 절차를 명시하는 등의 방법으로 이루어지도록 하고 있다. 그 방법의 제공에 있어서는 GDPR이나 CCPA와 거의 같다. 그러나 GDPR과 CCPA는 정보주체의 접근 및 열람의 편의성을 더욱 강하게 보장하는 방법을 취하여, 정보주체가 원하는 방식으로 정보주체의 권리행사에 관한 정보를 제공하도록 규정한다. 이러한 방식은 개인정보처리자가 제공하는 방법과 절차에 의해 정보주체가 열람권을 행사하도록 하는 우리나라 법과 크게 다른 점이다.

우리나라의 개인정보 보호법에서 어떤 경우에는 개인정보처리자가 마련한 방법과 절차를 따르도록 하고 있고, 어떤 경우에는 고시에서 정하는 바에 따라 요청 또는 답변을 하도록 하고 있다. 예를 들어, 고시 제3조 제6항 별지 제8호 서식 <개인정보 열람요구서>는 보호위원회를 통해 공공기관에 열람을 요구하는 경우에 사용하는 서식이고, 고시 제3조 제6항 별지 제9호 서식 <열람의 연기·거절 통지서>는 모든 개인정보처리자로 되어 있다. 이것은 시행령에서 규정하고 있는 것이기는 하지만, 열람요구서와 열람의 연기·거절 통지서의 적용 범위가 다른 것이 다소 혼란을 초래할 수 있다. 또한 공공기관이 아닌 일반 개인정보처리자의 경우 스스로 마련한 방법과 절차에 따라 열람 청구, 정정·삭제 청구를 받고 있는데, 열람 통지, 연기·거절 통지 등은 고시에서 정한 서식으로

하도록 하고 있다. 또한 이러한 서식에 따르지 않았을 경우 어떻게 되는지도 모호하다. 규제기관이 하나의 예시로 서식 등을 제시할 수는 있다. 하지만, 서식의 형식과 상관없이, 정보주체의 권리행사 등을 위해 필요한 항목 등의 내용을 서식에 반드시 포함하도록 하는 방식으로 개인정보 보호법에 규정하는 것이 바람직하다.

한편 우리나라 개인정보 보호법에서는 동의를 받을 때에만 정보주체에게 개인정보 수집·이용 목적 등 일부 내용을 고지하도록 하고 있는데, 다른 적법 근거(계약, 법률에 근거 혹은 정당한 이익 등)에 따라 개인정보를 수집할 경우에도 정보주체에게 관련 사항을 고지하도록 개선해야 할 것이다. 또한 고지하는 내용이 너무 제한적이므로 열람, 정정, 삭제권 등 정보주체가 행사할 수 있는 권리의 존재 및 권리행사 방법, 감독기관에 민원을 제기할 수 있는 권리 등 정보주체의 권리에 대한 내용들도 고지 내용에 포함되도록 하는 것이 바람직하고 필요하다.

정보주체에게 직접 개인정보를 수집하지 않는 경우, 우리나라 개인정보 보호법은 '정보주체의 요구가 있을 경우에만' 수집 목적 등 관련 내용을 알리도록 하고 있을 뿐만 아니라 동의가 아닌 다른 법적 근거에 의해 제3자에 제공되는 경우 제공하는 처리자 및 제공받는 처리자가 모두 관련 사항을 고지할 의무가 없다는 점도 문제이다. 또한 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자가 정보주체 이외로부터 개인정보를 수집하여 처리하는 때에는 개인정보의 수집 출처, 처리 목적, 개인정보 처리의 정지를 요구할 권리가 있다는 사실을 정보주체에게 알려야 하는데, 이 경우에도 정보주체의 동의를 받아 수집하는 경우에만 적용될 뿐이므로, SNS등 공개된 개인정보를 수집하거나 다른 적법 근거에 따라 다른 소스로부터 개인정보를 수집했을 경우에는 적용되지 않는 문제가 있다. 따라서 GDPR처럼 정보주체에게 직접 개인정보를 수집하지 않는 경우에도, 고지가 현실적으로 불가능한 예외적인 경우가 아니라면, 주요 개인정보 처리 내용을 고지하도록 개선할 필요가 있다.

더 나아가서 정보주체의 권리를 더욱 강하게 보장하고 그 행사를 실효성 있게 하기 위해서는 정보주체의 권리행사의 편의성을 더욱 높이는 방법과 절차를 강구해야 할 필요성이 있다. 급속하게 변화하는 디지털 환경에서 개인정보 처리 등 관련 정보와 권리에 대한 제공 방법 및 절차에 있어 정보주체의 가독성과 편의성을 높일 수 있도록 하는 방

안을 모색해야만 정보주체의 권리가 실효성 있게 보장될 수 있을 것이다. 개인정보 처리 방침 등을 사이트 홈페이지에 게시하고 있으나, 이러한 방식만으로는 정보주체의 권리보장 및 행사를 실효성 있게 하지 못한다. 정보주체가 가입하여 개인정보 처리 등에 대한 동의 절차 등을 거친 후에, 개인정보처리자가 정보주체에게 보장되어 있는 권리들을 쉽고 간단한 문구를 사용하여 이메일, 메시지, 앱의 알림 등 정보주체가 원하는 방법으로 알려주도록 강제하여야 한다. 그리고 이러한 권리 내용에 대한 제공은 그 권리와 관련된 사항이 발생했을 때 직접 관련되는 권리 내용을 고지하는 것은 물론이고, 정기적으로도 알려주도록 하는 방법도 강구할 필요가 있다. 또한 해당 정보주체가 자신의 권리 및 그 행사 등에 대해서 묻고, 이에 답변할 수 있는 방법(예를 들어, 상담 채팅 등의 활용)도 개인정보처리자에게 마련하도록 할 필요가 있다.

우리나라는 정보주체가 자신의 개인정보를 열람한 후에 정정권 및 삭제권을 부여하는 방식을 취하고 있다. 반면 GDPR, CCPA, 일본 개인정보 보호법 그 어디에도 그러한 방식을 취하고 있지 않다. 정정권 및 삭제권의 행사를 열람권의 행사를 전제로 할 경우, 정보주체의 권리행사에 넘어야 할 장애물을 하나 더 설치하는 것과 같은 효과를 가지게 되므로 이를 개선하는 것이 바람직하다.

우리나라는 정보주체가 자신의 개인정보 처리의 정지를 요구할 수 있는 조건을 제한하고 있지 않으며, 처리 전체에 대한 정지 및 처리의 일부 정지도 가능하게 하고 있다. GDPR은 정보주체의 처리에 대한 제한권은 처리자가 개인정보를 보유는 하며 개인정보의 처리 전체를 하지 못하도록 하고, 제18조 제1항 (a)호부터 (d)호까지에 해당하는 경우 처리 제한권을 부여하고 있다. 우리나라의 처리정지권이 GDPR보다 넓게 인정되고 있다. 하지만, 그러한 처리정지권이 현실적으로 거의 활용되고 있지 않다는 점이 문제로 지적된다. 따라서 이러한 정보주체의 처리정지권도 앞서 논한 것과 마찬가지로, 그 행사 및 방법을 실효성 있도록 하는 절차와 내용이 필요하다.

또한 GDPR은 정보주체의 삭제권, 처리 제한권 행사의 예외로 “법적 권리의 확립, 행사 또는 방어를 위한 경우”를 규정하고 있다. 이러한 예외 규정은 우리나라에도 도입할 필요가 있는 것으로 보인다.

제3절 정보주체의 개인정보 이동권

개인정보 이동권은 정보주체가 자신의 개인정보를 보유하고 있는 한 IT업체 등에서 다른 업체 등으로 이동할 수 있도록 정보주체에게 권리를 주는 것으로, 데이터 산업의 활성화와 경쟁 강화 및 새로운 서비스산업 등의 창출을 위한 맥락에서 고안된 것으로 볼 수 있다. 하지만 디지털 환경에서 데이터 산업의 발전과 확대에 따라 개인정보 침해의 위험도 함께 증대할 것이라는 점을 쉽게 예상할 수 있다.

GDPR은 개인정보 이동권의 행사가 삭제권을 침해하지 않아야 한다고 규정한다(제20조 제3항). 그러나 일반적으로 개인정보 이동권의 행사는 정보주체가 한 처리자로부터 탈퇴하여 개인정보를 삭제하고, 다른 처리자로 옮기는 방법으로 실현하는 것을 상정한 것이다. 우리나라 개인정보 보호법에서는 개인정보 이동권에 대한 규정이 마련되어 있지 않고, 신용정보법에서만 규정하고 있다(2021년 2월 4일 시행). 그리고 신용정보법은 신용정보주체가 해당 개인신용정보의 정확성 및 최신성이 유지될 수 있도록 정기적으로 같은 내역의 개인신용정보를 전송하여 줄 것을 요구할 수 있다는 점(제33조의2 4항)에서, 기존 처리자에 의한 처리와는 별개로 마이데이터 사업자에 대한 통합 처리 및 개인정보 유통을 고려하여 둔 규정이라는 것을 알 수 있는데, 이 점에서 GDPR이 상정하고 있는 모델과 큰 차이가 있다.

GDPR은 프로파일링 등에 의해 추론되거나 파생된 개인정보를 개인정보 이동권의 대상에서 제외함으로써 위험성을 줄이고자 하며, 특히 컨트롤러에게 일반적으로 완전성 및 기밀성에 따라 적절한 기술적, 조직적 수단을 이용해 무허가 또는 불법적인 처리와 돌발적인 손실, 파괴 또는 손상으로부터의 보호를 비롯한 개인정보의 적절한 보안을 보장하도록 하는 의무를 지움으로써 개인정보 침해의 위험성을 실효성 있게 막고자 한다.

CCPA는 개인정보 이동권을 접근권의 하나로 인정하고, 개인정보 이동권의 대상이 되는 개인정보를 이동권을 청구하는 시점에서 12개월 전까지 수집된 정보에만 한정하는 제한을 가함으로써 일정부분 개인정보 침해 위험성을 줄이고자 한다. 또한, 정보주체가 개인정보를 받아서 그것을 다른 기업에 방해 없이 자유롭게 전송할 수 있도록 하고, GDPR처럼 한 기업에서 다른 기업으로 바로 전송되게 할 의무까지는 인정하지 않음으로써 정보주체인 소비자의 개입과 결정권을 강화하고 있는 것으로 보인다.

우리나라는 신용정보법에서만 GDPR과는 취지를 달리하는 개인신용정보의 전송요구권을 규정한다. 우리나라도 4차 산업혁명에 따른 데이터 산업의 활성화 및 경쟁 강화를 표방하고 있다. 또한 그에 따른 개인정보 침해의 위험성도 증대된다. 그러나 개인정보 보호법에 일반적인 개인정보 이동권 및 규제에 관한 규정을 마련하지 않음으로써, 개인신용정보와 직접 관련이 없는 데이터 산업에서의 개인정보 전송 등에 대한 개인정보 침해의 위험에 대해 정보주체의 권리가 보장되지 못하는 한계와 문제점을 가지게 될 수 있다.

따라서 GDPR의 정보주체의 개인정보 이동권에 관한 규정과 CCPA의 일부 규정을 토대로 개인정보 보호법에 일반적인 정보주체의 개인정보 이동권을 보장하고, 그에 따른 개인정보 침해에 대한 실효성 있는 방지 및 사후규제에 관한 규정을 마련해야 한다.

제4절 프로파일링 및 자동화된 의사결정과 개인정보 주체의 권리

알고리즘의 자동화된 의사결정 과정에는 우선순위 결정, 분류, 관련짓기, 필터링이라는 일련의 과정이 존재하게 된다. 이 과정에서 인간의 개입에 따른 오류와 편향성, 검열의 가능성 등과 같은 본질적인 차별적 성격이 투입될 수도 있게 된다. 따라서 편향적인 데이터와 이를 통해 학습한 인공지능 알고리즘이 만들어내는 부정적인 결과인 차별, 편견, 배제 등을 효과적으로 규제하고 교정할 수 있는 방안들도 함께 모색되어야 할 필요성이 제기된다.

GDPR은 제22조에서 정보주체에게 프로파일링을 포함해 자동화된 처리만을 바탕으로 한 결정으로서 자신과 관련한 법적 영향 또는 이와 유사하게 중대한 영향을 미치는 결정의 대상이 되지 않을 권리를 인정하고 있다. 또한, 프로파일링 및 자동화된 의사결정에 관련된 개인정보 처리와 관련된 정보를 제공받을 권리를 두고 있으며, 부정확한 개인정보에 기반한 프로파일링 및 자동화된 의사결정에 대한 수정권, 삭제권(잊힐 권리), 프로파일링 등에 관련된 개인정보의 처리에 대한 제한권, 거부권 등도 인정된다.

우리나라의 개인정보 보호 법제에는 프로파일링 및 자동화된 의사결정에 대한 직접적인 정의 규정은 마련되어 있지 않다. 개인정보 보호법에서는 ‘처리’란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공,

공개, 파기, 그 밖에 이와 유사한 행위를 말하는 것으로 정의하고 있다(제2조 제2호). 신용정보의 이용 및 보호에 관한 법률(신용정보법)에서는 ‘처리’란 신용정보의 수집(조사를 포함), 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 결합, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 말하는 것으로 정의하고(제2조 제13호), ‘자동화평가’란 신용정보회사 등의 종사자가 평가 업무에 관여하지 아니하고 컴퓨터 등 정보처리장치로만 개인신용정보 및 그 밖의 정보를 처리하여 개인인 신용정보주체를 평가하는 행위를 말하는 것으로 정의한다(제2조 제14호).

개인정보 보호법에서는 프로파일링 및 자동화된 의사결정에 관한 규정은 전혀 없으며, 신용정보법은 신용정보와 관련해서만 부분적으로 자동화평가를 규정하고 있을 뿐이다. 신용정보법은 자동화평가는 기본적으로 가능하고 단지 자동화평가와 관련된 설명을 요구하고 추가 정보를 제공할 권리만을 인정하고 있다. 이에 인적개입을 요구할 권리의 여지는 볼 수가 없다. 또한 신용정보주체의 자동화된 평가가 모두 GDPR 제22조의 의미에서 ‘법적 영향을 발생시키거나 이와 유사하게 중대한 영향을 미치는 자동화된 처리’인지, 아니면 GDPR보다 폭넓게 규제하고자 하는 것인지는 모호하다. 더욱 큰 문제는 처음부터 신용평가 자체가 정보주체의 동의 없이 이루어지고 있다는 점이다. 마찬가지로 신용정보법은 정보주체의 권리에 대해 사전에 정보주체에게 고지할 의무를 포함하고 있지 않다.

개인정보의 보호를 위한 일반법이자 기본법이라고 할 수 있는 개인정보 보호법에서 인공지능시스템으로 인한 개인정보 침해 문제를 규율할 수 있는 기초적인 규범조차 마련되어 있지 않은 것은 커다란 문제라고 생각한다. 우리나라의 개인정보 보호 법제에서 프로파일링 및 자동화된 의사결정에 대한 직접적인 규정이 마련되어 있지 않기 때문에, 이에 대한 정보주체의 권리 인정 및 감독기관의 감독규제에 한계와 공백을 초래하게 될 것이다. 따라서 GDPR의 프로파일링 및 자동화된 의사결정에 관한 개념 및 정보주체의 권리 규정을 참조하여 우리나라 개인정보 보호 법제에 마련해야 할 것으로 보인다.

제5절 동의제도 개선 방안

현행 동의 제도가 지나치게 복잡하고 현실성이 없다고 비판하며 개선해야 한다는 주장이 제기되고 있다. 현행 동의제도의 문제점으로는 동의 절차가 형식적이라는 점, 사물

인터넷과 같은 기술환경에 적용하기 힘들다는 점, 지나치게 엄격하고 복잡하다는 점 등이 제기된다.

형식화되어 있는 현행 동의제도를 개선하기 위해서는 우선 정보에 기반한 동의(informed consent)를 실질화하는 방안을 모색할 필요가 있다. 중요한 내용은 단순하고 명확하게 전달하면서도 원하는 사람은 찾아볼 수 있도록 전체 정책에 접근하는 방법을 제공할 수도 있다. 중요한 것은 정보주체에게 실질적이고 효율적으로 정보를 제공하는 방법을 모색해야 한다는 것이다. 이와 병행하여 소비자단체, 개인정보 보호위원회, 소비자보호원 등 전문기관들이 주요 개인정보처리자들의 약관이나 개인정보 처리방침이 문제가 있는지 사전에 검토함으로써 불공정한 개인정보 처리방침으로 인한 피해를 방지할 수 있다. 현행 동의제도를 포괄동의로 전환하자거나 사전규제를 없애자는 제안도 있지만, 이것이 어떻게 정보주체의 보호로 이어지는지 납득하기 어렵다. 사후적으로 개인정보 오남용에 대해 강력히 제재하자는 것은 사전 동의제도와 양립할 수 없는 것이 아니다.

둘째, 동의 외에 개인정보 수집을 위한 다른 적법 근거를 활용할 필요가 있다. 예를 들어 계약 이행을 위해 필수적인 정보라면 추가적인 동의를 요구하지 않아도 무방할 것이다. 우리나라 개인정보 보호법 제15조는 GDPR과 유사하게 동의 외에도, 개인정보의 수집 및 처리를 위한 적법 근거를 제공하고 있다.법률 규정 혹은 법령상 의무(제15조 제1항 제2호), 공공기관의 소관업무 수행을 위해 불가피한 경우(제3호), 계약의 체결 및 이행(제4호), 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 경우(제5호), 개인정보처리자의 정당한 이익(제6호) 등이다.

이처럼 동의 외에 다양한 적법 근거를 인정하기 위해서는 몇 가지 전제가 필요하다. 우선 서비스 제공을 위해 필수적인 개인정보의 경우 계약의 체결 및 이행 조항을 수집 근거로 활용하더라도 필수적이지 않은 정보를 수집하고자 한다면 동의 등 다른 법적 근거가 필요하다. 민감정보 및 고유식별정보에 대한 별도의 동의 요건은 유지되어야 한다. 정보주체에 대한 고지 의무도 강화될 필요가 있다. 또한 동의가 아닌 다른 법적 근거에 따라 개인정보가 수집 및 처리되더라도 개인정보 처리와 관련된 정보들을 정보주체에게 제공하도록 개인정보 보호법이 개정되어야 한다. 더불어 동의에 기반할 경우 정보주체가 언제든지 동의를 철회할 수 있는 것과 같이, 정보주체의 동의에 기반하지 않을 경우에는 정보주체가 언제든 개인정보의 처리를 반대하거나 처리정지를 요구할 수 있는 권리를 보

장해야 한다.

셋째, 사물인터넷이나 자율주행자동차와 같이 만일 일일이 동의를 받는 것이 불가능한 경우는 어떻게 해야 할까? 현재로서는 어떠한 결론을 내리기 이전에, 새로운 기술이나 서비스가 기존의 동의제도와 어떻게 충돌하는지 추가적인 연구가 필요해 보인다. 구체적인 근거 없이 동의제도를 회피하기 위한 목적으로 사물인터넷 등의 새로운 기술환경이 근거로 활용되어서는 안 된다. 사물인터넷 환경이 도래할 것이므로 옵트아웃 방식으로 전환하자는 주장은 지나친 논리적 비약이다.

넷째, 법 위반 행위에 대한 강력한 처벌 등 동의 이외에 개인정보 보호를 위한 사회적 통제의 강화도 제안되고 있다.당연히 정보주체의 권리를 보호하기 위한 방안은 동의제도에 한정되어서는 안 된다. 개인정보 처리의 전 과정에서 개인정보를 안전하게 보호하고 개인정보처리자의 책임성을 강화할 수 있는 법제가 구축될 필요가 있으며, 이와 관련된 기술적인 보호 조치들도 수반되어야 할 것이다.

제5장 개인정보처리자의 책임성 강화

제1절 컨트롤러, 프로세서, 공동 컨트롤러의 개념과 책임 강화

GDPR은 컨트롤러와 프로세서, 공동 컨트롤러 개념을 정의하고, 그 구분기준을 구체화해 나가고 있는데, 이는 우리 개인정보 보호법에서도 수용할만한 점이다. GDPR은 개인정보파일의 처리 목적과 방법을 결정하는 자를 컨트롤러로 보고, 실제로 그 자가 개인정보파일에 접근하거나, 해당 개인정보파일을 처리하지 않더라도 그에게 컨트롤러로서의 책임을 부과하고 있는데, 우리나라의 경우는 개인정보파일의 운용도 타인에게 지시하였다면 그 자는 개인정보처리자로 볼 수 없고, 해당 지시자는 개인정보 보호법과 관련해서는 어떤 의무도 부담하지 않게 되는데, 이는 오늘날 개인정보를 처리하는 업무를 전문으로 하는 서비스가 확산되는 현실에서 권한과 책임이 상응하는 것으로 보기 어렵다. 그래서 우리 법제에도 개인정보처리자의 개념을 명확하게 하고, 실질적으로 개인정보 처리에 대한 결정을 하는 자에 대해서 책임을 부담할 수 있도록 처리자의 개념을 현재의 운용자보다는 완화하는 것이 바람직하다. 아울러 처리자의 구별기준을 명확하게 하면서, 이

를 현실에 부합하도록 끊임없이 구체화하는 노력이 이루어질 필요가 있다.

또한 우리나라 법제에도 공동개인정보처리자라는 개념을 도입할 필요가 있다. 현행 법제상으로도 공동개인정보처리자가 인정되지 않는다고 보기는 어려울 수도 있지만, 공동개인정보처리자 개념을 도입하면서, 공동개인정보처리자 상호의 책임이나 역할 등을 명료하게 규율하고 정보주체에게 알리도록 하여 투명성과 책임성을 강화할 필요가 있다.

아울러 우리나라 개인정보 보호법은 GDPR과 달리 개인정보 처리자가 개인정보 처리를 위탁하는 경우의 요건과 절차 및 책임성과 투명성을 보장할 수 있는 규율이 매우 빈약하다. 따라서 우리나라 법제에도 개인정보를 대신 처리하도록 하는 경우의 요건과 절차 및 책임성과 투명성을 보장할 수 있는 규율을 신설할 필요가 있다. 우리나라 개인정보 보호법은 위탁 처리시의 손해배상 책임에 대하여 수탁자를 위탁자의 소속 직원으로 본다고 하여 사용자책임의 요건을 충족하는 경우에만 위탁자가 책임을 부담하는 것으로 규정하고 있는데, 이런 태도는 GDPR이 컨트롤러에게 많은 책임을 부여하고 있는 것과 비교하여 개인정보 처리자의 책임을 지나치게 약화시키는 태도이다. 따라서 우리 법제에도 개인정보 처리위탁의 민사상 손해배상 책임에 대해서도 책임성을 강화하는 방향으로 개선할 필요가 있다.

제2절 안전조치를 취할 책임과 설명과 입증 의무

우리 개인정보 보호법에도 개인정보처리자에게 기술적, 조직적 조치를 취할 의무를 부과하는 규정이 있는데(개인정보 보호법 제29조), 기술적, 조직적 조치 의무의 범위가 '분실, 도난, 유출, 위조, 변조 또는 훼손되지 아니하도록' 하는 것에 국한되는 것으로 오인될 가능성이 있다. 개인정보 보호법에서 명확하게 모든 개인정보 처리에 대하여 안전조치 의무가 있다는 내용이 포함되도록 하는 것이 바람직하다.

개인정보 보호법은 내부 관리계획 수립, 접속기록 보관 등을 열거하면서, 대통령령으로 안전성 확보에 필요한 기술적, 관리적, 물리적 조치를 두도록 하고 있다. 개인정보 보호위원회는 열거된 조치에 대해서 '최소한의 기준'이라고 규정하고 있지만, 실질적으로는 열거된 조치에 준하는 책임을 다하면 보호 의무를 다한 것으로 해석될 소지가 충분하다. 따라서 오해의 소지를 없앨 수 있도록, 안전조치의 범위를 포괄적으로 표시하고,

기술적, 조직적 조치의 범주와 내용도 그에 부합하도록 수정할 필요가 있다.

또한 우리 법제에도 설명 및 입증의무(accountability)를 도입하여, 법률 준수를 위해 적절한 기술적, 조직적 조치를 취하고 있다는 것을 입증할 수 있는 조치를 취할 의무를 도입하는 것이 바람직할 것이다. 그리고 적절한 기술적, 조직적 조치의 판단기준을 '처리의 성격, 범위, 맥락 및 목적과 자연인의 권리와 자유에 대한 가능성과 심각성의 정도가 다양한 위험'을 고려한다는 점을 분명하게 규정하여 위험수준에 기반한 접근방법을 명시할 필요가 있다. 더불어 GDPR과 같이 적절한 기술적, 조직적 조치를 필요시 검토하고 갱신되어야 한다는 점을 분명하게 규정할 필요가 있다.

제3절 개인정보 처리의 보안에 관한 규정

우리 개인정보 보호법에도 이 법을 준수하여 개인정보의 처리가 될 수 있도록 처리의 모든 영역에서 보안과 관련된 안전조치를 취할 책임이 처리자에게 있다는 것을 명시할 필요가 있다. 그 내용으로는 위험에 대한 적절한 수준의 보안을 보장하기 위해 적절한 기술적, 조직적 조치를 이행할 의무가 있다는 점을 명시하여 위험기반 접근을 도입하는 것이 바람직할 것이다. 아울러 판단기준에는 최신 기술, 실행 비용, 처리의 성격, 범위, 맥락 및 목적, 그리고 처리가 자연인의 권리와 자유에 대해 갖는 가능성과 심각성의 정도가 다양한 위험을 고려하도록 하는 것이 좋을 것이다. 아울러 전송 또는 보관되거나 달리 처리되는 개인정보의 우발적 또는 불법적 파괴, 손실, 변경, 무단 공개나 그에 대한 접근 등 개인정보 처리에서 드러나는 위험을 특히 고려할 것을 규정할 수 있을 것이다.

적절한 수준의 보안을 보장하기 위한 적절한 기술적, 조직적 초치의 내용도 범주별로 구체화할 수 있다. 그 예시로는 개인정보의 가명화와 암호화, 처리 시스템 및 서비스의 지속적인 기밀성, 무결성, 가용성 및 복원력을 보장하는 능력, 물리적 또는 기술적 사고가 발생했을 경우 적시에 개인정보의 가용성과 접근성을 복원하는 능력, 처리 보안을 보장하기 위한 기술적, 조직적 조치의 효과를 정기적으로 시험, 평가, 감정하는 절차를 둘 필요가 있다. 그리고 승인된 행동강령이나 승인된 인증 메커니즘을 준수하는 것이 보안에 대한 적절한 기술적, 조직적 조치를 취한 것임을 입증하는 요소로 사용될 수 있다는 점도 규정하면 좋을 것이다.

제4절 설계에 의한 개인정보 보호와 기본설정에 의한 개인정보 보호

우리나라의 개인정보 보호법에는 설계에 의한 개인정보 보호나 기본설정에 의한 개인정보 보호에 관한 규정이 없다. 그 뿐만 아니라 개인정보처리자의 안전조치 의무도 협소하게 규정하고 있고, 보안과 관련한 안전조치 의무도 다소 형식적으로 규정되어 있기 때문에 개인정보 보호를 위한 수단이 통합된 개인정보 처리가 이루어지도록 하는 사전 규율이 미비하고, 신기술에 조응하는 개인정보 보호에도 취약하다. 이런 점을 고려한다면 설계 및 기본설정에 의한 개인정보 보호는 개인정보처리자의 책임 조항과 결합하여 매우 효과적인 사전예방의 수단이 될 수 있을 것이다.

개인정보 보호 설계를 할 때 고려할 사항으로 최신 기술, 실행 비용, 처리의 성격, 범위, 맥락 및 목적, 그리고 처리가 자연인의 권리와 자유에 대해 갖는 가능성과 심각성의 정도가 다양한 위험을 고려하도록 하는 것이 바람직할 것이다. 설계에는 개인정보 보호 법제가 요구하는 모든 사항을 준수해야 하고, 정보주체의 권리를 보호할 수 있는 조치를 포함해야 한다. 해당 기술적, 조직적 조치는 정보 최소화 등 개인정보 보호 원칙을 효과적인 방식으로 구현하고 필요한 보호조치를 처리에 통합하도록 설계해야 하며, 가명화 같은 조치도 포함된다는 점을 명시할 필요가 있다. 설계를 통해서 처리에 통합된 조직적, 기술적 조치의 적절성을 판단하는 시점은 처리 수단 결정 시점과 실제 처리 시점이 되어야 한다는 점도 분명하게 규정해야 한다. 아울러 이를 준수하는 하나의 방안으로 인증 메커니즘을 활용할 수 있다. 개인정보 감독기관은 인증 시에 해당 인증 메커니즘이 설계에 의한 개인정보 보호를 준수하는지를 포함시키도록 하고, 이를 검토하여 승인함을 통해서 구체화시킬 수 있을 것이다.

아울러 기본설정에 의한 개인정보 보호 규정도 도입할 필요가 있다. 특히 인터넷과 관련해서는 기본설정을 통해 개인정보가 개인의 개입 없이 무제한 수의 자연인이 접근 가능하게 되지 않도록 보장할 필요가 있다.

제5절 개인정보보호 영향평가

우리 개인정보 보호법에도 민간분야에서도 개인정보 영향평가를 시행할 수 있도록 할 필요가 있다. 모든 민간분야에서 개인정보 영향평가를 수행하도록 하는 것보다는 고위험

을 불러올 가능성이 있는 경우로 제한하여 운용할 수 있을 것이다. 고위험을 불러올 가능성이 있는 경우로는 GDPR에서 규정하는 예시를 참조할 수 있다. 즉, (i) 프로파일링 등의 자동화된 처리에 근거한, 개인에 관한 개인적 측면을 체계적이고 광범위하게 평가하는 것으로 해당 평가에 근거한 결정이 해당 개인에게 법적 효력을 미치거나 이와 유사하게 개인에게 중대한 영향을 미치는 경우나 (ii) 특정범주의 개인정보에 대한 대규모 처리나 범죄경력 및 범죄 행위에 관련된 개인정보에 대한 처리에 해당하는 경우, (iii) 공개적으로 접근 가능한 지역에 대한 대규모의 체계적 모니터링의 경우 등이다.

어떤 경우에 영향평가가 필요할지를 명확한 문구로 규정하기는 쉽지 않다. 영향평가가 필요한 기준을 변화하는 신기술이나 새로운 서비스와 관련하여 적절하게 공개하는 것은 많은 도움이 될 것이다. 그래서 우리 법제에도 개인정보 보호위원회에 영향평가가 필요한 경우에 대한 지침을 제정할 수 있는 권한을 부여할 필요가 있다. 이와 관련하여 유럽연합에서 제시한 10가지의 기준이나, 영국 ICO의 기준, 프랑스 CNIL의 기준 등도 참고할 가치가 있다.

개인정보 영향평가는 개인정보처리자가 개인정보를 처리하기 이전에 하는 것이 정상이다. 그러나, 개인정보의 처리 작업으로 초래되는 위험에 변화가 있을 때에도 영향평가가 필요할 수도 있으므로 이에 대한 규율을 할 필요도 있다. 또한 개인정보 영향평가가 포함해야 할 최소한의 내용을 규정할 필요가 있다. 여기에는 (i) 예상되는 처리 작업 및 개인정보처리자의 정당한 이익 등 개인정보 처리의 목적에 대한 체계적인 설명, (ii) 목적과 관련한 처리 작업의 필요성 및 비례성에 대한 평가, (iii) 개인정보주체의 권리와 자유에 대한 위험성 평가, 개인정보주체와 기타 관련인의 권리 및 정당한 이익을 고려하여 개인정보의 보호를 보장하고 본 규정의 준수를 입증하기 위한 안전조치, 보안조치, 메커니즘 등 위험성 처리에 예상되는 조치도 포함되어야 한다.

또한 GDPR에서와 같이, 개인정보처리자로 하여금 상업적 이익이나 공익의 보호 또는 처리 작업의 보안을 침해하지 않고, 예정된 처리에 대한 개인정보주체 또는 그 대리인의 의견을 구해야 한다는 규정을 도입할 필요가 있다. GDPR은 개인정보 영향평가에도 불구하고 위험을 억제하는 적절한 수단을 갖추지 못한 경우에는 개인정보 감독기관에게 사전 자문을 구하게 하는 절차를 두고 있는데, 개인정보 보호법에도 해당 규정을 도입할 필요가 있다. 예정된 개인정보 처리가 초래하는 위험을 파악하고, 그에 대한 위험 억제 수단

을 적절하게 갖추지 못한 경우에는 개인정보 보호위원회가 조치를 취할 수 있도록 할 수 있다. 이 규정을 도입하게 되면 고위험이 예상되는 개인정보 처리는 해당 처리가 도입되기 전에 개인정보 영향평가를 거쳐야 하고, 위험이 존재한다면 개인정보 보호위원회와의 사전협의를 거쳐야 하므로, 위험을 파악하고 통제할 수 있는 것으로 평가된 서비스만이 제공될 수 있게 하는 역할을 한다.

특히, 사전 자문 시에 ① 가능한 경우, 처리에 관여하는 컨트롤러, 공동 컨트롤러 및 프로세서의 개별 책임, 특히 사업체집단 내의 처리에 대한 책임, ② 예정된 처리의 목적 및 방법, ③ 본 규정에 따라 개인정보주체의 권리와 자유를 보호하기 위해 제공되는 조치 및 안전조치, ④ 가능한 경우, 독립 정보보호 책임자(DPO)의 상세 연락처, ⑤ 개인정보 영향평가, ⑥ 감독기관이 요청한 기타 정보를 제공하도록 하는 규정도 함께 도입할 필요가 있다.

제6절 개인정보처리자의 처리 활동 기록 의무

우리 개인정보 보호법은 GDPR과 달리 개인정보 처리방침에 기재하는 내용은 인터넷의 홈페이지를 통해서 일반 공개를 하도록 하고 있다. 반면 GDPR은 일반 공개가 아닌 요청 시 제공할 의무로 규정하고 있다. 따라서 처리 활동 기록 의무를 범위를 나누어서 일반에게 공개할 사안과 일반에게 공개되는 것이 불합리한 사안에 대해서는 요구에 따른 제공 의무로 두는 것이 바람직해 보인다.

예를 들어 개인정보 보호를 위한 안전조치의 내용은 일반 공개로 하는 경우, 오히려 보안을 취약하게 할 수도 있기 때문에 일반 공개보다는 요청 시 제공으로 하는 것이 적정할 수 있다. 개인정보 수집의 목적 등은 널리 일반 공개를 하더라도 문제가 없을 수 있다. 따라서 처리의 내용을 기록하도록 하되, 일반 공개의 대상과 요구 시 제공의 대상으로 나누는 것이 좋을 것이다.

제7절 개인정보 침해 통지 제도

우리 개인정보 보호법은 개인정보 유출통지에 대한 규정을 두고 있는데, 대체로 GDPR의 규정과 대동소이하다. 양자의 가장 큰 차이는 GDPR은 모든 개인정보 침해를 통지의

대상으로 하지 않고, 위험 발생의 우려를 기준으로 하고 있는데 반하여 우리 개인정보 보호법은 침해 통지를 하지 않아도 되는 경우를 규정하지 않고 있다.

제8절 독립 정보보호 책임자(Data Protection Officer)

우리 개인정보 보호법에서도 CPO에 해당하는 '개인정보 보호책임자' 아니라, 독립적인 지위에서 감독과 조언 및 정보제공을 할 수 있는 '독립 정보보호 책임자(DPO)'를 도입할 필요가 있다. 이 경우 기존의 개인정보 보호책임자 규정은 폐지하고, DPO를 신설하는 것이 바람직할 것이다. 왜냐하면 CPO에 해당하는 개인정보 보호책임자는 굳이 개인정보 보호법에 규정하지 않아도 기업에서는 당연히 선임하는 직책이기 때문이다.

DPO를 선임하도록 의무를 도입한다면, 이를 모든 기업에게 선임 의무를 부과하는 것보다는 위험성이 높은 방식으로 개인정보를 처리하거나, 위험성이 높은 개인정보를 처리하는 경우에만 선임할 의무를 부과하는 것이 바람직할 것이다. GDPR의 경우와 같이, 개인정보처리자의 핵심 활동(core activities)이 정보주체에 대한 대규모의 정기적, 체계적 모니터링을 필요로 하는 처리 작업으로 구성되는 경우로 규정할 수도 있을 것이다. 공공기관이나 공적 업무를 수행하는 조직인 경우는 규모와 관련 없이 선임의 필요성이 있다. 다만, 이 경우는 여러 조직을 통합하여 DPO가 지정될 수 있게 할 수 있다. 기업의 경우에도 다수의 계열사를 포괄하여 단일한 DPO를 지정할 수 있도록 허용할 수 있다.

DPO는 전문성을 갖는 자로 선임하도록 할 필요가 있고, 그에 대한 자격증과 인증기관에 대한 규정도 마련하는 것이 좋을 것이다. 이와 관련해서는 현재의 CPO 포럼과 같이 개인정보처리자를 회원으로 하고 CPO들의 협의체와 같은 성격을 갖는 조직은 독립성을 가진 것으로 보기 어려우므로, 이들 보다는 DPO들이 구성하는 협회 등을 통해서 해당 업무가 이루어질 수 있도록 할 필요가 있다.

DPO의 지위와 관련해서는 (i) 관여 보장 - 개인정보 보호와 관련한 모든 문제에, 적시에 적절한 방식으로 관여할 수 있도록 보장하고. (ii) 필요한 자원 제공과 지원의무 - DPO가 업무를 수행할 수 있도록 해당 업무와 개인정보 및 처리 작업에 대한 접근을 수행하고, 전문지식을 유지하는 데 필요한 자원을 제공하여 DPO를 지원하도록 해야 한다. 또한 (iii) 지시 금지 보장, (iv) 불이익 금지. (v) 직접 보고. (vi) 정보주체의 연락가능성.

(vii) 이해충돌 금지, (viii) 기밀 보호 의무 등을 규정할 필요가 있다.

DPO의 업무로는 (i) 정보와 조언 제공 - 정보처리를 하는 자들에게 자신들의 의무에 대한 정보와 조언 제공, (ii) 모니터링과 감사, 교육, (iii) 개인정보 영향평가에 관한 조언 제공, (iv) 감독기관과의 협력과 연락 업무 등을 규정할 수 있다.

제9절 개인정보 보호 행동강령과 인증 등과 관련하여 자율규제의 촉진과 그 조건

우리나라의 자율규제 단체는 자율규제 규약을 자율적으로 제정하는데, 해당 자율규제 규약이 개인정보 보호법에 조응하는 것인지 여부에 대한 판단을 받는 구조가 마련되어 있지 않다. 아울러 해당 단체에 소속된 개인정보처리자는 자율규제 규약을 준수할 의무도 없다. 게다가 자율규제 단체나 독립된 인증기관이 규약의 준수 여부를 모니터링하는 구조도 갖추고 있지 않다. 따라서 현재 우리나라의 자율규제는 아무런 구속력이 없는 순수한 자율규제의 유형으로 볼 수 있다. 그런데, 이러한 순수 자율규제의 유형보다는 자율규제 규약에 대한 승인 제도를 두고, 만약 승인된 자율규제 규약을 채택하여 개인정보 보호법 준수에 대한 외부적인 인증의 효과를 누릴 수 있도록 하려면, 자율규제 규약에 대한 승인절차를 두는 것이 좋을 것이다. 이 경우, 자율규제 규약이 개인정보 보호법에 부합하는지 여부를 개인정보 보호위원회에 승인을 신청하여 승인을 받을 수 있는 절차를 둘 필요가 있다. 개인정보 보호위원회는 해당 자율규제 규약이 개인정보 보호법에 비추어 타당하다고 인정되는 경우에는 승인을 하고 이를 공고하게 된다.

현재 우리나라의 자율규제에는 공정성을 담보할 수 있는 독립적이고 전문적인 자율규제 모니터링 기관이 존재하지 않는다. 우리도 자율규제 규약의 준수 여부를 감독하고 모니터링할 수 있는 제도를 마련할 필요가 있는데, 이 모니터링 기관은 해당 개인정보처리자로 구성된 협회나 단체 또는 해당 개인정보처리자로부터 독립성이 있어야 하고 전문성을 갖추어야 한다. 이 모니터링 기관에는 각 개인정보처리자에 대한 권리구제 신청 등에 대응하여 권리구제를 처리할 수 있는 권한도 부여되는 것이 좋다. 한편, 각 개인정보처리자가 자율규제 규약을 준수하지 않을 경우 인증을 취소하여야 한다.

현재 우리 법제상 ISMS 인증은 특정한 요건에 해당하는 기업에게 법률상 인증을 받도

록 인증제도가 운용되고 있다. 반면, PIMS는 자발적인 참여에 바탕을 둔 인증제도이다.

우리나라에는 인증과 관련하여 독립적이고 전문적인 모니터링 수행기관이 없다. 그런데, 인증제도가 신뢰받기 위해서는 인증에 대한 모니터링을 수행할 기관이 신뢰할 수 있어야 하고, 독립적이고 전문적인 능력을 갖춘 곳이어야 한다. 그런 점에서 현재의 구조는 심사기관의 독립성을 신뢰하기 어려운 구조이다. 예를 들어 한국정보통신진흥협회는 정보통신서비스 제공자 및 정보통신망과 관련된 사업을 경영하는 자로 구성된 협회이다. 따라서 독립적이고 전문적인 모니터링 기관을 통한 모니터링이 이루어질 수 있도록 제도를 개선하는 것이 바람직할 것이다.

제6장 범죄예방과 수사 등 분야에서 개인정보 보호

제1절 GDPR의 적용 예외로서 '범죄수사 등'

GDPR은 "범죄의 예방, 수사, 적발 또는 기소, 형사제재의 집행 그리고 공공의 안전에 대한 위협의 방지 및 그 위협으로부터 공공의 안전의 보호를 목적으로 관할기관에 의해 이루어지는 개인정보의 처리"에는 적용되지 않는다. 대신에, 유럽연합은 GDPR 제정과 같은 날 '범죄수사 등'의 영역에서 개인정보 보호를 위하여 회원국들이 적용해야 할 지침으로 DIRECTIVE (EU) 2016/680(일명 '경찰 디렉티브')를 제정하였다. GDPR과는 달리 디렉티브는 법적 강제력은 없지만, EU 회원국은 범죄수사 등의 영역에 적용되는 국내입법에서 디렉티브에 규정된 내용을 반영해야 한다.

여기에서 디렉티브의 적용대상이 되는 '관할기관'이란 범죄의 예방, 수사, 적발 또는 기소, 형사제재의 집행 그리고 공공의 안전에 대한 위협의 방지 및 그 위협으로부터 공공의 안전의 보호에 권한이 있는 모든 공공기관뿐만 아니라, 그러한 목적을 위해 공적 권한을 행사할 수 있도록 회원국 법이 권한을 부여한 그 밖의 기구나 기관을 포함한다. 디렉티브의 주된 적용대상은 경찰일 것이다. 범죄의 예방이나 수사를 위한 경찰의 활동은 어떤 사건이 형사범죄인지 여부가 아직 불확실한 단계에서 관련 개인정보를 수집하는 경우도 포함한다. 여기에는 형사소송법이나 경찰 직무에 관한 법령에 규정된 바에 따라 강제조치 권한을 행사하는 것도 당연히 포함된다. 그리고 수사 외에 범죄의 예방이라든

가 공공의 안전에 대한 위협에 대응하기 위한 경찰활동도 포함된다. 회원국의 법체계에서 경찰 등 법집행기관에 범죄수사 등의 목적에 필수적이지 않은 다른 업무권한을 부여한 결과 그와 같은 업무의 수행을 위하여 개인정보를 처리하는 경우가 있을 수 있는데, 이때는 GDPR의 적용을 받는다.

제2절 GDPR과의 차이점 분석

1. 개인정보 처리원칙

가. 투명성 원칙의 적용 제한(디렉티브 제4조)

GDPR 제5조(1)(a)는 개인정보 처리의 원칙으로 적법성, 공정성과 투명성을 규정하고 있는 반면에, 디렉티브 제4조(1)(a)는 적법성과 공정성을 규정하면서 투명성 원칙은 명시적으로 규정하지 않는다. 범죄수사 등을 위해서는 비밀수사라든가 비디오감시와 같이 비밀리에 개인정보를 수집하는 활동이 허용될 수 있어야 한다는 이유에서이다. 물론 그처럼 비밀리에 수행되는 개인정보 수집활동도 적법성의 원칙에 따라 명확한 법적 근거를 갖추어야 하고, 필요최소한도의 수집에 그쳐야 한다.

나. 정보의 삭제 또는 보관의 기한 제한(디렉티브 제5조)

디렉티브의 적용영역에서 정보주체의 삭제요청권과 컨트롤러의 삭제의무는 GDPR보다 제한적이다. 개인정보의 처리가 디렉티브 제4, 8, 10조에 따른 회원국의 법규정을 침해하거나, 컨트롤러의 법적 의무를 이행하기 위하여 개인정보가 삭제되어야 하는 경우에 한하여 정보주체의 삭제권(그리고 컨트롤러의 삭제의무)이 인정된다(디렉티브 제16조(2)).

다. 범죄와 관련하여 정보주체의 범주의 구별(디렉티브 제6조)

범죄의 예방이나 수사, 기소, 형집행 등의 영역에서는 피의자나 피해자 등 정보주체의 범주를 분명하게 구별하여 개인정보를 처리하는 것이 매우 중요하다. 이에 따라 디렉티브의 적용영역에서 회원국은 컨트롤러에게 가능한 한 정보주체의 범주를 (a) 범죄를 저질렀거나 저지르려 한다고 믿을 만한 상당한 이유가 있는 사람, (b) 유죄판결이 확정된

사람, (c) 범죄피해자 또는 일정한 사실로 볼 때 범죄피해자라고 믿을 만한 근거가 있다고 인정되는 사람, (d) 그 밖의 사람들, 예를 들어, 수사절차나 이후의 형사절차에서 진술을 위하여 소환될 가능성이 있는 사람, 범죄에 관한 정보를 제공할 수 있는 사람, (a)와 (b)에 해당하는 사람의 지인이나 동료 등으로 명확하게 구별하여 개인정보를 처리해야 한다.

라. 정보의 정확성 ; 사실에 근거한 개인정보와 평가적 의견에 기초한 개인정보의 구별 (디렉티브 제7조)

형사절차에서는 개인정보를 포함하는 진술들은 대개 진술자의 주관적인 인식에 기초한 것이라는 점에서 객관적인 사실증명이 항상 가능한 것은 아니라는 특수성을 고려해야 한다. 디렉티브는 사실에 근거한 개인정보와 평가적 의견에 기초한 개인정보를 명확하게 구별할 것을 요구한다(제7조(1)).

마. 개인정보 처리의 적법성(디렉티브 제8조)

디렉티브 제8조(1)에 따르면, 회원국은 EU법이나 회원국 법에 근거가 있고, 범죄수사 등 디렉티브 제1조 (1)에 규정된 목적을 위하여 관할기관이 수행하는 직무집행에 필요한 범위에 한해서만 개인정보의 처리가 적법하도록 규정해야 한다. 그리고 디렉티브의 범위에 속하는 개인정보의 처리에 관한 회원국 법은 최소한 개인정보 처리의 목적과 처리되는 개인정보의 범위를 구체적으로 규정해야 한다(제8조(2)).

경찰·검찰 등 법집행기관은 범죄의 예방·수사·기소 등의 직무를 수행하는데 필요한 개인정보를 제공하도록 개인에게 요구하거나 명령할 권한을 가진다. 그러한 경우에 정보주체의 동의는 개인정보 처리의 법적 근거가 될 수 없다.

바. 특수 범주의 개인정보의 처리(디렉티브 제10조)

디렉티브 제10조는 범죄수사 목적의 민감정보 처리에 관하여 GDPR보다 비교적 완화된 요건 하에 폭넓게 용인하는 태도를 취한다. (a) EU법이나 회원국 법이 허용하는 경우 ; (b) 정보주체나 타인의 생명을 보호하기 위한 경우 ; 또는 (c) 개인정보의 처리가 정보주체가 명백하게 공개한 개인정보와 관련된 경우로서, '엄격하게 필요한 경우에 한해

서’ 그리고 정보주체의 권리와 자유에 대한 적절한 보호조치가 보장되어야 한다는 조건에서 회원국은 범죄수사의 목적을 위한 민감정보의 처리를 허용할 수 있다. 민감정보의 처리에 대하여 정보주체의 명시적인 동의가 있는 경우에는 민감정보의 처리가 가능하도록 법규정을 두어야 하지만, 정보주체의 동의 그 자체만으로는 범죄수사 목적의 민감정보의 처리가 정당화될 수 없다(전문 37).

사. 자동화된 개별 의사결정(디렉티브 제11조)

위와 같은 디렉티브 제11조(1)과 (2)의 내용을 자동화된 의사결정의 적용을 받지 않을 권리를 정보주체의 권리로 규정하고 있는 GDPR 제22조와 비교해 보면, 몇가지 차이가 발견된다. 첫째, 디렉티브 제11조에서 원칙적으로 금지되는 자동화된 의사결정은 ‘불리한’ 법적 효력 또는 중대한 효과를 미치는 경우에 한정된다. GDPR 제22조에는 ‘불리한’이라는 문구가 없다. 둘째, 자동화된 의사결정이 허용되는 예외사유는 EU법이나 회원국 법에 법적 근거가 있을 것과 EU법이나 회원국 법이 정보주체의 권리와 자유를 위한 적절한 보호조치를 제공할 것을 요건으로 하는데, 이는 GDPR 제22조(2)(b)와 유사하긴 하나 ‘정보주체의 정당한 이익’을 위한 보호조치는 제외되어 있다는 점에서 다소 완화되어 있다. 셋째, 민감정보에 근거한 자동화된 의사결정에 대해서도 디렉티브는 GDPR 제22조(4)보다 완화된 요건 하에 폭넓게 허용하는 태도를 취하고 있다. 한편, 프로파일링이 디렉티브 제10조에 규정된 민감정보를 근거로 하여 개인에 대한 차별의 결과를 낳는다면 이는 EU법에 따라 금지되어야 한다(제11조(3)).

2. 정보주체의 권리 보장 관련

가. 정보주체의 권리행사를 위한 통지(디렉티브 제12조)

범죄수사 등 목적의 개인정보 처리에 적용되는 디렉티브는 GDPR보다 투명성원칙을 제한적으로 적용하는 경향을 보이고 있는바, 이에 따라 디렉티브 제12조(1)에서는 “투명한 방식의 제공”이라는 문구가 제외되어 있다. 그리고 정보주체가 그 권리에 입각해서 컨트롤러에게 일정한 요청을 하는 경우에 GDPR은 ‘부당한 지체 없이, 요청을 접수한 후 1개월 이내에’ 그 요청에 따라 취해진 조치에 관한 정보를 정보주체에게 제공하도

록 규정하고 있는 반면에, 디렉티브는 '요청을 접수한 후 1개월 이내'라는 엄격한 제한을 두지 않는다는 점에서 차이가 있다(디렉티브 제12조(3)).

또한 GDPR 제12조(4)는 컨트롤러가 정보주체의 요청에 대응한 조치를 취하지 않은 경우에 그 이유와 불복할 권리에 대해 정보주체에게 고지해야 할 의무를 규정하고 있는데, 디렉티브에는 이에 상응한 컨트롤러의 고지의무에 관한 일반 규정이 존재하지 않는다. 디렉티브 제13~16조가 정보주체의 권리에 대한 제한조치를 허용하고 있음을 감안하여 디렉티브는 GDPR 제12조(4)과 같은 일반적인 고지의무를 규정하지 않는 대신에, 개별적인 경우에 불복할 권리에 관한 고지의무를 별도로 규정하는 방식을 채택하고 있다.

나. 컨트롤러의 개인정보 수집시 정보제공(디렉티브 제13조)

디렉티브에서는 제13조가 GDPR 제13조, 제14조에 상응하는 규정인데, 몇가지 중요한 차이점이 있다. 첫째, 디렉티브 제13조는 컨트롤러가 개인정보를 수집한 원천이 정보주체 본인인지 아닌지에 따른 구별을 두지 않는다.

둘째, 디렉티브 제13조 제1항과 제2항은 컨트롤러가 정보주체에게 제공해야 할 정보의 내용과 범위를 열거하고 있는데, GDPR에서 컨트롤러의 제공의무로 규정된 것보다 약간 축소되어 있다.

셋째, 디렉티브는 회원국이 아래와 같은 사유를 근거로 하는 경우에 관련 개인의 기본권과 정당한 이익을 적절하게 고려하면서 민주사회에서 필요한 적절한 한도에서 제13조 제2항에 따른 정보의 제공을 연기·제한·생략하는 입법조치를 취할 수 있다고 규정한다(제13조(3)) : (a) 공식적 또는 법적 탐문, 수사나 절차에 대한 장애의 방지, (b) 범죄의 예방, 탐지, 수사, 소추, 또는 형사제재의 집행에 대한 장애의 방지, (c) 공공의 안전의 보호, (d) 국가의 안전의 보호, (e) 다른 사람들의 권리와 자유의 보호.

다. 정보주체의 접근권의 보장과 제한(디렉티브 제14, 15조)

접근할 수 있는 정보의 범위에서 미세한 차이가 있기는 하지만, 범죄수사 등의 목적으로 이루어지는 개인정보 처리에 대해서도 정보주체의 접근권을 보장해야 한다는 점은 GDPR 제15조와 동일하다. 그런데 GDPR에서 정보주체의 접근 요구가 있는 경우에 처리가 진행 중인 개인정보의 사본을 제공하도록 규정하고 있는 것과는 다르게, 디렉티브에

는 그러한 규정이 없다. 디렉티브 전문에 의하면, 정보주체가 디렉티브에 의하여 부여되는 권리를 행사할 수 있도록 처리가 진행 중인 개인정보에 대한 '전체 요약(full summary)'을 제공해도 충분하다고 한다(전문 43). 무엇보다 큰 차이는 접근권에 대한 제한조치가 넓게 허용된다는 점이다. 디렉티브 제15조는 회원국의 법체계에서 관할기관이 범죄수사 등의 목적으로 개인정보를 처리하는 경우에 정보주체의 접근권을 제한할 수 있도록 허용한다.

라. 정정・삭제・처리제한권의 보장과 제한(디렉티브 제16조)

GDPR이 정보주체의 권리로 규정한 정정권(GDPR 제16조), 삭제권(제17조), 처리제한권(제18조)는 원칙적으로 범죄수사 등 목적의 개인정보 처리에서도 적용되어야 한다(디렉티브 제16조). 다만, 범죄수사 등의 목적으로 관할기관이 개인정보를 처리하는 경우에는 정보주체의 동의에 의한 수집은 원칙적으로 의미가 없으며 투명성원칙의 적용이 제한적일 수밖에 없다는 점에서, 디렉티브에서 규정한 삭제권과 처리제한권의 근거사유에 관한 규정은 GDPR과는 다소 차이가 있다(디렉티브 제16조(2), (3)). 특히 개인정보의 삭제권은 사실상 회원국의 법령이 디렉티브에 따라 개인정보 처리의 합법성의 기준으로 규정한 것을 위반한 경우 또는 개인정보를 삭제할 의무를 부과하고 있는 경우에만 인정된다는 점에서 GDPR이 규정한 삭제권보다 훨씬 제한적이다. 또한 디렉티브는 정보의 정확성에 대한 이의가 제기되었고 그 정확성 여부가 확정되지 않은 경우와 증거사용을 목적으로 개인정보를 보존할 필요가 있는 경우에는 컨트롤러로 하여금 삭제 대신에 처리제한을 하도록 규정한다(제16조(3)(b)).

마. 감독기구를 통한 권리 행사(디렉티브 제17조)

회원국은 하나 이상의 감독기관을 두고 경찰 디렉티브의 준수를 자문 및 감독하여야 하며, 감독기관들은 국내외적으로 다른 감독기관들과 상호 협력 및 지원할 수 있어야 한다. GDPR에 따라 회원국에 이미 설립된 감독기관이 있다면 이 디렉티브에 따라 설립될 감독기관이 수행해야 할 업무에 대해 소관하도록 맡길 수 있다(전문 76; 제41조제3항).

경찰 디렉티브의 감독기관은 GDPR과 그 독립성, 구성, 설립, 주무 권한에 대한 규정이

대체로 유사하다. 다만 경찰 디렉티브 감독기관의 권한은 전반적으로 GDPR에 비하여 축소하여 규정되었다. 우선 조사권과 관련하여서 감독기관의 자료 접근권(power to obtain access)만을 남기고 자료제출 명령권(power to order)을 규정하지 않았으며, 개인정보 보호 감사의 형태로 조사를 수행할 권한, 정보 관리자나 처리자에게 규정 위반 혐의를 통지할 권한, 정보 처리 장비 및 수단에 대한 접근권을 포함하는 부지 접근권 등이 삭제되어 있다. 또 시정조치와 관련해서 정보 관리자나 처리자에게 견책 처분을 내릴 권한, 정보주체의 권리행사 요청에 응할 것을 명령할 권한, 개인정보 침해사실을 정보 주체에게 알리도록 명령할 권한, 개인정보 정정 또는 삭제나 처리 제한을 명령하고 개인정보를 공개받은 수령자에 대한 조치 통지를 명령할 권한, 제3국이나 국제기구의 수령자에 대한 정보 흐름 중단을 명령할 권한 등이 규정되어 있지 않다. 자문권과 관련하여서는 공익을 위한 정보 관리자 업무 수행에 대한 사전 허가 권한이 삭제되었다. 경찰 디렉티브는 외부적인 감독을 제한하는 한편으로 소관 기관 내부적으로 디렉티브 침해에 대한 기밀 보고를 장려하기 위한 체계를 갖추도록 규정하였다(제48조).

제3절 우리나라의 수사 영역에서 개인정보 보호와 통제에 관한 규율과 제도적 개선방안

현행 개인정보 보호법은 범죄수사 및 형집행과 관련한 개인정보 처리에 대해서 많은 예외 규정을 두고 있으며, 이에 수반하는 감독 또한 미흡하게 이루어지고 있다. 우선 현행 개인정보 보호법은 제18조제2항에서 공공기관이 보유한 개인정보에 대하여 수사기관이 범죄수사를 위해서 필요로 하는 경우나 구금시설이 형(刑) 및 감호, 보호처분의 집행을 위하여 필요로 하는 경우 특별한 요건이나 절차 없이도 목적 외로 제공하도록 하였으며, 이러한 제공 및 처리 대상에 민감정보와 고유식별정보도 광범위하게 포함되어 있다. 범죄수사 및 형집행 등과 관련된 개인정보파일의 경우 감독기관에 대한 등록 및 공개가 면제되어 있고 개인정보 처리방침도 수립 및 공개 의무가 없어 개인정보 보호 감독에서 전면적으로 제외되어 있다. 정보주체의 열람 및 정정·삭제권과 처리정지권의 행사, 정보주체의 고지받을 권리 역시 동반하여 제한되어 있어 정보주체의 권리 침해에 대한 인지와 권리구제가 상당히 어려운 상황이다. 또한 경찰은 구체적인 법령적 근거에 의

하지 않고 상당히 방대한 개인정보 처리 시스템을 구축·운영해 왔다.

제7장 국가인권기구와 개인정보 보호

제1절 개인정보 보호 감독의 규범

한 국가의 개인정보 보호 감독 체계는 일반적으로 개인정보 보호법의 준수를 감독하는 법제도 및 기관을 아우르는 개념으로, 국제적으로 여러 규범에서 독립적이고 효과적인 하나 이상의 개인정보 보호 감독기관(Data protection authorities)의 설치를 권고하고 있다.

개인정보 보호 감독 체계에 대한 국제 규범이 등장한 것은 컴퓨터를 비롯한 현대 정보통신기술의 발달로 개인정보의 처리가 자동화됨에 따라 보다 적극적으로 개인정보 보호 관련 법률과 규제 체계를 수립할 필요성이 확인되었기 때문이다. 특히 개인정보 보호 체계에서 독립적인 감독기관이 요청되는 이유는 공공기관에 대한 감독과 효과적인 규제 측면에서 살펴볼 수 있다. 전통적으로 정부기관이나 대기업들이 개인정보를 대량으로 처리하는 상당부분을 차지하였고, 이들의 개인정보 처리에 대해서 전문적으로 평가·견제할 수 있는 장치가 필요했다. 따라서 감독자와 피감독자가 조직적·기능적으로 분리되어 있는 것이 중요하다. 또 개인정보 보호 감독기관이 효과적이기 위해서는, 감독기관이 믿을 수 있는 규제자(credible regulator)라는 점에 대해 시민과 기업의 신뢰가 확보되어야 한다. 투명하고 공정한 임명과 면직절차는 감독기관이 조직적으로 자율적이라는 점을 보증할 수 있고 그리하여 이해관계자들로부터 신뢰를 확보할 수 있다.

특히 유럽의 개인정보 보호 감독기관들은 디지털 시대 감시자(the watchdogs of the digital age)의 역할을 기대받으며, 특히 유럽사법재판소는 완전히 독립적인 개인정보 보호 감독기관을 기본권의 '수호자'(the guardians)로 지칭하였다. 유럽연합 기본권청은 개인정보 보호 감독기관의 독립성이 국가 개인정보 보호 시스템에 대한 국민의 신뢰 측면에서 중요하다고 지적하였다. 개인정보 보호 감독기관의 독립성에 대한 의구심이 계속되거나 감독기관들이 주어진 임무를 효율적이고 효과적으로 수행하기에 충분한 자원을 확보하고 있지 못한 것처럼 보인다면, 국민들은 개인정보 보호나 프라이버시에 대한 자

신들의 우려가 진지하게 다루어지고 있다고 믿지 못할 것이다.

개인정보 보호 감독에 대한 국제 규범을 적극적으로 주도해 온 유럽은 유럽연합과 유럽평의회의 관련 규범을 일치시켜 가면서 유럽 지역 내 개인정보 보호 감독이 같은 방식으로 작동하게끔 노력하였다. 특히 유럽 각국 국내 이행 법률들 간 불일치와 결점을 보완하기 위하여 유럽연합 집행위원회는 개인정보 보호 개혁 패키지를 마련하였다.

2016년 5월 24일 발효한 유럽연합 개인정보 보호 개혁 패키지(EU Data Protection Reform package)는 두 가지 법안을 포함하고 있다. 그 중 하나는 <일반 개인정보 보호 규정(General Data Protection Regulation, GDPR)>이다. '규정'이 유럽연합 회원국에 직접 구속력을 갖는다는 점에서 이 제안은 유럽 전체적으로 개인정보 보호에 대한 포괄적 입법체계와 통합형 수행체계를 마련한 것으로 평가된다. 개혁 법안의 다른 하나는 <형사법집행 목적의 개인정보 보호에 대한 디렉티브(directive on protecting personal data processed for the purpose of criminal law enforcement, 일명 '경찰 디렉티브')>이다.

특히 GDPR의 경우 개인정보 보호 감독기관에 대한 규정 측면에서 주요한 변화가 있었다고 평가받는다. 과거 개인정보 보호 디렉티브 요건을 따르면서도 독립성 요건을 훨씬 더 구체적으로 규정하고 감독기관의 설립 및 구성, 설립에 대한 규칙 등이 법률상으로 강화되었다. 직무와 권한 또한 상세하게 규정하고 강화하였다. 특히 주감독기관을 두어 역내 집행체계를 일원화하는 한편으로, 감독기관 간 협력 및 차이에 대한 해결 규정을 두었다.

유럽연합 경찰 디렉티브는 법집행기관의 특수성 측면에서 GDPR에 비하여 감독기관의 업무와 권한을 다소 제한한 측면이 있으나, 경찰 등 법집행 기관에 대해서도 원칙적으로 개인정보 보호 원칙 및 독립적인 감독을 적용하도록 하였다는 점에서 개인정보 보호 감독을 강화하였다는 의미가 있다.

유럽평의회의 경우 개인정보 처리 관련 규범에서 경찰 및 형사사법을 포함한 모든 분야를 망라하고 있다는 점에서 유럽연합과 차이를 보이고 있다.

우리나라의 경우, 2020년 8월 5일 개인정보 보호법이 개정 시행되면서 개인정보 보호위원회가 독자적인 조직·인사·예산의 운영 권한을 갖는 국무총리 소속의 장관급 중앙행정기관으로 격상되면서 그 독립성이 강화되었다. 그러나 현행 개인정보 보호 감독 체계는 여전히 다음과 같은 규제 사각 지대를 방치하고 있다는 점에서 한계가 있다.

첫째, 개정 개인정보 보호법 및 신용정보법에 따르면 금융회사는 개인정보 보호위원회의 감독 대상에서 제외된다. 금융회사의 신용정보 이용과 보호를 동시에 소관하고 있는 금융위원회는 독자적인 중앙행정기관이기는 하지만 개인정보 보호 감독 기능이 매우 취약하다. 금융위원회처럼 업종별 규제기관이 개인정보 보호와 충돌하는 업무를 함께 수행하는 경우 소관 행정부처와 관련 업계의 이해관계나 압력으로부터 자유롭지 못할 가능성이 높다.

둘째, 현행 개인정보 보호법은 국가안전보장과 관련한 개인정보 처리에 대해서 포괄적으로 그 적용을 제외하는 규정을 두고 있다. 이는 유럽연합 GDPR이 국가안전보장(national security)을 위한 목적으로 일부 적용을 제한하되 그 제한은 입법 조치를 통해서만 가능하도록 규정한 것과 큰 차이가 있다. 이 입법 조치들은 개인정보 처리자의 의무 및 정보주체의 권리에 상응해야 하며, 그러한 제한이 기본권과 자유의 본질을 존중할 뿐 아니라, 해당 조치가 민주 사회에서 필요하고 비례적인 조치인 경우에 한한다. 또한 적절한 경우 최소한 (a) 처리 또는 처리 범주의 목적 (b) 개인정보의 범주 (c) 도입되는 제한의 범위 (d) 남용이나 불법 접근 또는 전송을 방지하기 위한 보호장치 (e) 컨트롤러 또는 컨트롤러 범주에 대한 상세설명 (f) 처리 또는 처리 범주의 성격, 범위 및 목적을 고려한 보관 기간과 적용 가능한 보호장치 (g) 정보 주체의 권리와 자유에 대한 위험 (h) 제한에 대한 고지를 받을 정보 주체의 권리(단, 고지가 제한의 목적에 해를 미칠 수 있는 경우는 제외)에 관한 구체적 규정을 포함해야 한다). 특히 2013년 이후 유엔에서 국가의 통신 감시, 감청 및 개인정보 수집에 대해 적절한 투명성과 책무성을 보장할 수 있는 독립적이고 효과적인 국내 감독 체계를 설립하거나 운영할 것을 각국에 요청해 온 점을 고려하였을 때, 국가안전보장과 관련한 개인정보 처리에 대해서도 반드시 독립적이고 효과적인 감독 체계가 마련되어야 한다.

셋째, 범죄의 수사 및 형의 집행 관련 개인정보 처리의 광범위한 예외를 두고 있다. 궁극적으로는 이를 보완하는 입법적인 개선이 이루어져야 하겠지만, 이 분야 정보주체의 권리구제를 방대한 예외 상황 속에 방치할 수 없는 상황임을 고려하여 볼 때, 현행 제도 속에서 국가인권기구의 기능을 통해 가능한 감독 방안을 모색해 볼 필요가 있다. 특히 국가인권위원회가 침해 조사 및 구제의 주요 대상인 구금・보호시설 및 수사기관의 개인정보 침해 사건에 대한 조사 및 구제 활동을 보다 강화한다면, 현행 개인정보 보호법에

서 광범위하게 제외되고 있는 범죄수사 및 형집행 관련 개인정보 처리에 대한 권리구제가 보완될 수 있을 것이다.

제2절 인권기구의 개인정보 보호 활동

유럽연합 인권기구인 기본권청(FRA)은 개인정보 보호 감독기관, 평등기구, 국가인권기구를 3대 기본권 아키텍쳐(the fundamental rights architecture)로 지칭하며 이들 기본권 옹호기구들의 밀접한 협력 속에 인권 증진의 시너지 효과를 추구해야 한다고 보았다.

유럽연합 개인정보 보호 감독기관(EDPS) 또한 국제적인 규범에 따라 설립된 개인정보 감독기관과 국가인권기구들의 상호작용이 향후 점차 일치되고 예측가능한 형태를 띨 것이라고 보았다. 개인정보 감독기관은 완전한 독립성과 외부 영향 회피 원칙 하에 구속되지만 이러한 원칙이 두 기관 간 협력을 제지하지는 않을 것이라고 한다.

기본권청은, 유럽지역의 인권기구이면서 개인정보 보호와 관련한 주요한 정책에 대하여 의견을 내고 정책적으로 개입해 왔다. 이는 기본권청이 유럽 기본권헌장의 사생활권과 개인정보 보호권을 기본적으로 소관하고 있기 때문이기도 하지만, 기본권청의 법적 임무인 “특수주제에 관한 결론 및 견해의 공표” 대상에 “정보 사회, 특히 사생활 및 개인정보 보호 문제”가 포함되어 온 데 기반한 것이다. 기본권청의 경우 “빅데이터, 알고리즘 및 차별”에 대한 보고서 등 신기술 분야 사생활 및 개인정보 보호 문제를 주목하는 연구 및 자료 발표를 계속해 왔고, GDPR의 준수 및 감독과 직접 관련한 연구 및 자료 또한 계속 발표해 왔다는 점이 시사적이다.

특히 최근 코로나19의 지구적 확산 속에 코로나19 감염병 위기에 대응하기 위해 취해진 민관의 다양한 조치들이 사생활권과 개인정보 보호권 등 기본권에 중대한 영향을 미침에 따라 인권기구와 개인정보 보호 감독기관 간 협력과 상호작용 노력이 눈에 띈다.

또한 최근 유엔 등 국제인권기구 및 각국 국가인권기구들은 인공지능에 대한 인권적 접근과 규제 체제 논의를 이끌고 있다. 특히 공공부문 의사결정에 사용되는 인공지능에 대하여 차별금지법 등 인권관련 법과 규범에 근거한 개입과 권리구제 요구가 커지고 있으며, 인권영향평가 등 이 분야 국가인권기구의 역할과 개입에 대한 기대 또한 커지고 있다.

우리의 국가인권위원회 또한 국제인권규범에 따라 설립된 국가인권기구로서 국가기관, 지자체의 인권침해에 대한 조사 및 구제, 인권정책 개선 권고 등을 소관해 왔고 차별 및 평등권 침해 행위에 대해서는 기업 등 사인에 대해서도 조사 및 구제 기능을 가지고 있다. 오랜 기간 차별 시정의 경험을 축적해온 국가인권위원회는 인공지능으로 인한 차별 시정 및 권리구제에 있어서 다른 기관보다 강점을 가지고 있다. 알고리즘 기반 의사결정의 정보인권 침해 문제는 개인정보 보호권 침해에 그치지 않으며 그 인권침해 및 차별에 대하여 국가인권기구의 종합적인 접근과 시정이 필요하다.

제3절 시사점

국제규범에 부합하는 효과적이고 독립적인 개인정보 보호 감독체계를 수립하기 위하여 신용정보법의 개인정보 관련 조항을 개인정보 보호법으로 일원화하고 금융위원회의 개인정보 감독권한을 개인정보 보호위원회로 이관하는 것이 바람직하다.

범죄수사 및 형집행, 국가안전 보장 목적의 개인정보 처리와 관련하여, 일정한 예외를 인정하더라도 개인정보 보호를 위한 구체적인 규정이 마련될 필요가 있으며 독립적인 감독이 이루어져야 한다. 특히 국가인권위원회가 침해 조사 및 구제의 주요 대상인 구금·보호시설 및 수사기관의 개인정보 침해 사건에 대한 조사 및 구제 활동을 보다 강화한다면, 현행 개인정보 보호법에서 광범위하게 제외되고 있는 범죄수사 및 형집행 관련 개인정보 처리에 대한 권리구제가 보완될 수 있다.

더불어 최근 국제적으로 인권침해 우려가 증가하고 있는 인공지능 기술에 대하여 각국 국가인권기구들의 보다 적극적인 역할이 요구되고 있다.

제8장 결론 및 정책권고

1. 정보주체의 권리 보호를 위한 정책 권고

가. 정보주체는 자신의 개인정보가 어떻게 처리되는지에 대해 고지 받을 권리를 가진다. 동의를 받을 때뿐만 아니라, 계약이나 정당한 이익 등 다른 적법 근거에 따라 개인

정보가 수집될 경우에도, 정보주체로부터 개인정보를 직접 수집한 때뿐만 아니라 간접적으로 개인정보를 획득할 경우에도 개인정보처리자는 정보주체에게 개인정보 처리와 관련한 정보를 제공해야 한다. 정보주체에게 제공되는 정보는 처리의 주체, 목적, 방법뿐만 아니라 정보주체가 어떠한 권리를 행사할 수 있는지, 자신의 권리가 침해되었을 때 어떻게 구제받을 수 있는지도 포함해야 한다.

나. 정보주체에게 개인정보의 처리와 관련한 내용을 고지할 때에는 정확하고, 투명하며, 이해하기 쉬운 형식으로 명확하고 평이한 언어를 사용하여야 한다.

다. 정보주체는 개인정보처리자가 보유하고 있는 자신의 개인정보에 대한 열람·정정·삭제권을 가진다. 그러나 정보주체의 정정·삭제권이 열람권 행사를 전제로 하는 것은 아니다.

라. 정보주체는 자신의 개인정보의 처리 방법, 처리 여부에 대해 알 권리를 가진다. 또한 자신이 동의한 개인정보의 처리에 대해서는 동의를 철회할 권리, 동의가 아닌 다른 법적 근거에 의한 개인정보의 처리에 대해서는 자신이 원하지 않을 경우 처리의 정지를 요구하거나 반대할 권리를 가진다.

마. 과학적 연구·통계 작성·공익적 기록보존 목적으로 개인정보를 가명처리하거나 가명처리된 개인정보를 활용하는 경우에도 정보주체의 권리는 존중되어야 한다. 다만, 정보주체의 권리를 보장하면 처리 목적의 달성이 불가능하거나 중대하게 손상되는 경우, 혹은 권리의 보장이 불가능하거나 매우 과도한 노력을 요하는 경우에 한하여 정보주체의 권리를 제한할 수 있다.

바. 정보주체는 개인정보처리자에게 제공한 자신의 개인정보를 체계적이고 기계 판독이 가능한 형식으로 제공받을 권리 및 다른 개인정보처리자에게 해당 개인정보를 이전할 권리(개인정보 이동권)를 가진다.

사. 정보주체는 프로파일링 등, 본인에 관한 법적 효력을 초래하거나 이와 유사하게 본인에게 중대한 영향을 미치는 자동화된 처리에만 의존하는 결정의 적용을 받지 않을 권리를 가진다. 또한 자동화된 의사결정의 유무, 관련한 로직과 정보주체에 미치는 중대한 영향에 대한 정보를 제공받을 권리를 가진다. 예외적으로 자동화된 의사결정이 이루어지는 경우 정보주체는 인적 개입 요구권, 의견 진술권, 이의제기권을 보장받아야 한다.

아. 이해하기 쉽고 평이한 문구를 사용하거나 아이콘 등을 활용하여 정보주체가 단순

하고 명확하게 중요 내용을 이해할 수 있도록 하는 등, 정보주체의 동의가 실질적으로 정보에 기반한(informed) 동의가 될 수 있도록 해야 한다. 소비자단체, 개인정보 보호위원회, 소비자보호원 등 전문기관들이 정보주체를 대신하여 주요 개인정보처리자의 약관이나 개인정보 처리방침에 문제가 없는지 검토하고 인증하도록 하는 것도 하나의 대안이 될 수 있다.

2. 개인정보 처리자의 책임성 강화를 위한 정책 권고

가. 개인정보처리자가 개인정보 보호법을 준수하고 이를 입증할 수 있도록 하는 책임성 규정이 개인정보 보호원칙에 반영되어야 한다.

나. 개인정보처리자는 개인정보 보호법을 준수하고 이를 입증할 수 있는 기술적, 조직적 조치를 취해야 한다. 이러한 조치의 수준은 개인정보 처리의 위험성에 비례(위험 기반 접근)해야 한다.

다. 이러한 기술적, 관리적 조치는 개인정보의 처리 방법을 결정한 시점 및 그 처리가 이루어지는 해당 시점에 이행되어야 하며, 개인정보 보호원칙을 효율적으로 이행하고 필요한 안전조치가 개인정보 처리에 통합될 수 있도록 설계되어야 한다(개인정보 보호 중심설계). 또한, 개인정보처리자는 특정 처리 목적에 필요한 최소한의 개인정보만 처리되도록 기본설정을 통해 적절한 기술적, 관리적 조치를 이행해야 한다(개인정보 보호 기본설정).

라. 개인정보처리자는 처리자의 신원, 처리의 목적, 처리되는 개인정보 등 처리 활동을 기록하고 보존해야 한다.

마. 개인정보 영향평가는 공공기관 뿐만 아니라 개인정보 처리의 위험성이 큰 민간분야로 확대되어야 한다. 영향평가의 수행 여부는 형식적인 기준이 아니라 실질적인 위험성을 기준으로 판단해야 하고, 개인정보 영향평가가 포함해야 할 최소한의 내용을 개인정보 보호법에 규정하며, 영향평가 과정에서 정보주체의 의견을 구하도록 한다. 영향평가에도 불구하고 위험을 억제하는 적절한 수단을 갖추지 못한 경우 개인정보 보호위원회에 자문을 구하도록 하는 절차를 둔다.

바. 현행 개인정보 보호법에서 규정하고 있는 개인정보 보호책임자와 별개로, 개인정

보 처리자로부터 독립적인 지위를 갖고 개인정보처리자를 자문하고 감독할 독립 정보보호 책임자(DPO) 제도를 도입할 필요가 있다. 공공기관 및 개인정보 처리 위험성이 높은 민간 기업을 대상으로 전문성이 있는 자를 DPO로 선임하도록 한다.

사. 자발적인 참여에 기반한 인증 제도를 도입하되, 인증기준과 인증기관에 대한 승인 및 관리는 개인정보 보호위원회가 담당한다. 또한 각 분야별 개인정보처리자들이 고유한 규범을 '행위 규범'으로 구체화하고 독립적인 모니터링 기관을 통해 준수 여부를 확인하는 행위 규범 제도를 마련할 필요가 있다. 이 역시 개인정보 보호법 준수를 입증하는 하나의 방식이 될 수 있다.

3. 신기술 환경에서 인권 보호를 위한 정책 권고

가. 과학적 연구와 통계 작성은 한 사회의 지식 기반을 확대하고 공공정책 및 산업발전에 유용하게 활용될 수 있다. 과학적 연구와 통계 작성을 목적으로 개인정보를 애초 수집한 목적 외로 활용할 필요성이 있으나, 개인정보의 목적 외 활용은 정보주체의 권리에 부정적인 영향을 미칠 수 있다. 따라서 과학적 연구와 통계 작성 목적은 정보주체의 권리 제한에 상응하는 공공적 가치를 가져야 한다. 해당 분야의 윤리 규범을 준수해야 하며, 그 결과물은 사회에 공유되어 모두가 향유할 수 있어야 한다.

나. 과학적 연구와 통계 작성 목적으로 안전하게 개인정보를 처리, 연계하기 위한 데이터 거버넌스 체제를 구축할 필요가 있다. 이는 과학적 연구의 공공적 가치를 판단하기 위한 심사위원회의 구성, 해당 목적을 위해 처리되는 개인정보 최소화를 위한 조치, 가명처리나 암호화를 포함하는 안전조치, 전송 및 보관 과정에서의 보안조치, 연구자에 대한 교육 및 훈련, 연구결과물이 개인정보를 침해할 우려가 없는지에 대한 검토, 개인정보 처리에 대한 공개 및 정보주체의 거부권 보장 방안 등을 포함한다.

다. 개인정보를 과학적 연구 및 통계 작성 등의 목적으로 애초 수집 목적 외로 추가 처리하더라도 데이터 최소화, 보관 제한 등 개인정보 보호원칙은 준수되어야 한다. 즉, 특정한 과학적 연구 및 통계 작성에 필요한 최소한의 개인정보만이 처리되어야 하고, 가능한 한 익명처리해야 하며, 특정 목적(특정한 과학적 연구 및 통계 작성 목적)이 다하면 해당 개인정보를 파기해야 한다.

라. 민감정보를 과학적 연구 및 통계 목적으로 활용할 경우, 법령에 근거해야 하고 해당 법률에서는 민감정보 처리에 필요한 안전조치를 규정해야 한다.

마. 인공지능 등 신기술은 개인정보 자기결정권 뿐만 아니라, 표현의 자유, 적법절차, 노동권, 평등권 및 차별받지 않을 권리 등 다른 기본권에 부정적 영향을 미칠 수 있다. 국가인권위원회는 신기술에 관한 법령, 제도, 정책, 관행의 인권적 영향에 대하여 적극적인 조사, 연구, 권고 또는 의견 표명에 나서야 한다.

바. 최근 인공지능이 그 개발이나 사용 과정에서 편향된 학습으로 인해 성별, 인종, 빈곤 지역에 따라 사람을 차별한 사례가 드러났으며 인공지능의 사용이 확산됨에 따라 차별이 확산·증폭될 위험성이 있다. 인공지능은 개발되거나 사용되는 과정에서 그 알고리즘 및 데이터셋이 헌법과 차별금지 관련 법률들 및 국가인권위원회법이 보호하는 평등권과 차별금지 원칙을 침해하지 않아야 한다. 국가인권위원회는 인공지능의 차별에 대한 조사 및 권리구제에 나서야 하며, 차별을 방지하기 위한 인공지능 알고리즘, 데이터셋 및 그 결과에 대한 검증 기준 및 감독 체계를 개발하고 교육 및 홍보하여야 한다.

사. 인공지능이 기본권에 미치는 부정적 영향을 최소화하기 위해 인권영향평가를 시행할 필요가 있다. 특히 법적 또는 이와 유사하게 중대한 영향을 미치는 자동화된 의사결정에 사용되거나 공공기관이 도입하는 인공지능의 경우 인권영향평가가 의무화되어야 한다. 국가인권위원회는 인공지능에 대한 인권영향평가의 대상, 시기, 기준, 이행 방안 등에 대한 정책을 개발하고 이를 교육 및 홍보하는 한편, 인권영향평가의 제도화를 위하여 노력하여야 한다.

아. 독립적 인권기구로서 사생활의 비밀과 자유, 개인정보 자기결정권 등 기본권을 옹호할 의무가 있는 국가인권위원회와 개인정보 보호법에 근거를 두고 설립된 개인정보 감독기관인 개인정보 보호위원회는 신기술 발전에 따라 국민의 기본권이 침해되지 않고 보호될 수 있도록 협력해야 한다.

4. 개인정보 보호체계 효율화를 위한 정책 권고

가. 신용정보법, 위치정보법의 개인정보 관련 조항을 개인정보 보호법으로 일원화하고 금융위원회의 개인정보 감독권한을 개인정보 보호위원회로 이관해야 한다.

나. 국제 규범과의 조화를 위해, 현재 유일하게 구속력 있는 개인정보 관련 국제규범인 유럽평의회 108호 협약에 가입할 필요가 있다.

다. 유럽연합과는 일본의 사례와 같이 상호 적정성 결정을 체결할 필요가 있다. 이를 위해서 일본과 같이 보완 규정에 의존하는 것보다는 우리 개인정보 보호법을 GDPR과 동등한 수준으로 개선할 필요가 있다. 또한 우리 국민의 개인정보가 다른 나라에서도 보호받을 수 있도록 다른 나라 개인정보 보호 법제에 대한 적정성 판단을 포함한 개인정보 국외 이전 제도를 개선할 필요가 있다.

5. 정보기관 및 수사기관의 개인정보 처리와 관련한 정책 권고

가. 현행 개인정보 보호법은 범죄의 수사와 공소의 제기 및 유지를 위하여 필요하거나 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우, 개인정보의 목적 외 이용·제공 제한, 민감정보 및 고유식별정보의 처리 제한, 개인정보파일의 등록 및 공개, 개인정보처리방침의 수립 및 공개에 대하여 일률적으로 그 적용의 예외를 두고 있다. 특히 이와 동반하여 정보주체의 열람 및 정정·삭제권과 처리정지권의 행사, 정보주체의 고지 받을 권리 또한 일률적으로 배제하고 있다. 수사기관 및 구금시설의 개인정보 처리에 대한 개인정보 보호법의 일률적인 예외 규정들은 법률적인 개선이 필요하며 개인정보 보호위원회가 독립적인 감독을 수행하도록 해야 한다.

나. 국가안전보장 목적으로 개인정보 보호 규범의 적용을 일부 제외하더라도, 개인정보 보호법 혹은 별도의 법률을 통해, 대상 개인정보의 수집·이용의 목적, 개인정보의 항목, 조치 업무 및 그 대상자의 범위, 안전성 확보 조치, 개인정보 처리자의 명시, 개인정보의 보유 및 이용 기간, 정보주체에 대한 고지와 권리 행사 및 예외 등에 관해 구체적으로 규정해야 한다.

다. 국가인권기구인 국가인권위원회는 수사기관 및 구금시설의 개인정보 처리 및 정보주체의 권리 행사에 있어 부당한 침해가 발생하지 않도록 고유의 조사 및 권고의 기능을 발휘하여 일정한 수준의 감독권을 행사할 필요가 있다.

제1장 서론

제1절 연구 목적 및 필요성

2020년 1월, 논란 끝에 개인정보 보호법을 비롯한 데이터 3법이 국회를 통과하여 8월 5일 시행되었다. 개인정보 보호법 체계는 국내 법제도로서의 정합성뿐 아니라 데이터의 국제적인 이동이 불가피한 세계화된 시장 환경에서 국제규범과의 조응이 중요한 과제이다. 특히, 유럽연합은 데이터의 해외 이전과 관련하여 적정한 수준의 개인정보 보호 법제를 갖추지 못한 국가로의 데이터 이전에 대해서 개입할 수 있는 규정을 두어 왔고(소위 '적정성 평가제도'), 이를 실제로 적용하여 데이터의 국외 이전을 제한하고 적정성 평가의 대상 범위를 실질적으로 넓혀 왔으며 4년마다 재평가를 받도록 하는 의무를 신설하는 등 이 제도를 점점 강화시켜 왔기 때문에 이는 매우 현실적인 문제이다. 게다가 유럽연합의 개인정보 보호 법제와의 적정성 평가를 마친 국가들도 유럽연합과 같은 적정성 평가제도를 법제에 포함하는 사례가 늘고 있어서, '적정성 평가제도'를 가진 국가들은 점점 더 많아지고 있다.

1980년 OECD의 <프라이버시 보호와 개인정보의 국제유통에 대한 가이드라인에 관한 이사회 권고>, 1990년 유엔의 <개인정보 전산화 가이드라인>은 세계적으로 개인정보 보호를 위한 규범이 되어 왔다. 이후 유럽은 이 분야 국제규범을 선도해 왔으며, 유럽연합의 개인정보 보호법(General Data Protection Regulation, 이하 GDPR)이 대표적이다. 한국 정부도 GDPR에 대한 적정성 평가를 현재 추진 중이고, 최근 현대화가 이루어진 유럽평의회(Council of Europe) 108호 협약에는 이미 옵저버로 가입되어 있다. 유럽 개인정보 보호 규범은 수십 년간 유럽사법재판소의 판결, 유럽인권재판소의 여러 결정을 통해 견고하게 자리 잡아 왔으며 최근 신기술 환경에서 정보주체의 권리를 효과적으로 보호할 수 있는 규범 수립을 위한 노력이 이어지고 있다. 유럽평의회가 108호 협약을 현대화한 주요 배경에는 최근 확산되고 있는 신기술 사용에 대응하여 개인정보 보호 규범을 개선하려는 이유가 있었으며[1], 유럽연합이 1995년 개인정보 보호 디렉티브(95/46/EC)를 개선

1) "the use of new information and communication technologies", https://www.coe.int/en/web/data-protection/convention108/modernised 참조.

하여 2018년 GDPR를 시행한 배경 중 하나도 인공지능 의사결정 등 신기술에 적절히 대응하려는 이유가 꼽힌다. 유럽 외 국가에서도 신기술 환경에서 개인정보 보호 관련 법률을 개선하는 문제를 최근 중요하게 다루어 왔다. 예를 들어 캐나다 개인정보 감독기관인 OPC(Office of the Privacy Commissioner of Canada)는 2020년 3월 13일 인공지능에 대한 규제를 고민하며 캐나다 민간부문 개인정보 보호법인 PIPEDA(Personal Information Protection and Electronic Documents Act)에 대한 개정 제안을 발표하였다. 이 개정 제안에는 PIPEDA에 인공지능, 자동화된 의사결정에 대한 정의를 포함시키는 등의 11가지 제안사항을 포함하고있다[2]. 반면, 한국에서 개인정보 보호법의 개정 과정은 개인정보 보호 규범의 강화보다는 신기술 발전을 위한 보호 규범 완화 취지에서 이루어졌다는 점에서 국가인권위원회나 시민사회에서 우려를 표해 왔다.

최근 우리나라의 개인정보 보호 법제 개정과 관련해서는 다음과 같은 연구가 절실하게 필요하다. 첫째, GDPR의 적정성 평가를 염두에 두고 진행되었다는 개인정보 보호 법제 개정이 과연 GDPR의 ‘적정성 평가’ 기준에 부합하는지를 검토, 평가할 필요가 있다. 이를 위해서 GDPR의 적정성 평가의 기준이 무엇인지를 검토해야 하고, 특히 유럽사법재판소의 슈렘스(Schrems) 판결 및 미국과의 프라이버시 쉴드(Privacy Shield) 추진하는 과정에서 제기되어 온 ‘적정성 평가’ 기준의 확장은 물론, 국가 감시 등과 관련한 법제와 적법절차 보장 등의 평가 기준 등에 대해서 검토할 필요가 있다. 둘째, 이를 바탕으로 우리나라의 개인정보 보호 법제가 적정성 평가의 기준에 부합하는지를 검토, 평가할 필요가 있다. 셋째, 단순한 ‘적정성 평가’의 수준을 충족하는 것 외에도 GDPR의 법제도와 관련하여 우리나라 개인정보 보호 법제의 미비점과 보완할 점을 검토, 평가하는 것도 필요하다.

아울러 이런 최근 국제규범 현황을 면밀하게 검토하여 신기술 환경에서 정보주체의 권리를 효과적으로 보호하기 위한 개인정보 보호 법제의 개선 연구도 필요하다. 최근 몇 년간 세계적으로 연구자, 기업, 시민사회, 정부, 국제기구 등 다양한 주체들이 인공지능 등 신기술과 관련된 윤리 가이드라인을 발표해 왔는데, 프라이버시 및 개인정보 보호는

2) OPC(2020), “Consultation on the OPC’s Proposals for ensuring appropriate regulation of artificial intelligence”, <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/pos_ai_202001/>.

대부분의 인공지능 원칙 문서에서 포함하고 있는 주제이다. 이들 원칙 문서들을 살펴보지 않더라도 최근 몇 년 동안 신기술 환경에서의 사생활의 권리와 개인정보 보호 문제는 국내외를 막론하고 핵심적인 이슈가 되었다. 사물인터넷(IoT)을 통해 기존에는 수집되지 않았던 엄청난 규모의 데이터가 수집되고, 정형·비정형의 '빅데이터'로부터 새로운 가치를 창출하기 위한 분석 기술이 발전하고 있다. 인공지능의 훈련 단계와 활용 단계 모두에서 데이터의 흐름은 필수적이다. 신기술이 활용하는 모든 데이터가 개인정보는 아니지만, 개인정보는 데이터의 핵심적인 부분을 이룬다. 언론에 자주 회자되는 "개인정보는 4차 산업혁명의 원유"라는 표현은 개인정보에 대한 기업들의 요구를 단적으로 드러내고 있다. 반면 이와 같은 신기술의 발전은 개인정보 자기결정권을 심각하게 위협할 수도 있다. 유럽연합의 제29조 개인정보 보호작업반(WP29)은 사물인터넷은 "눈에 잘 띄지 않는 방식으로 구석구석에 편재하는(pervasive) 서비스를 제공"하기 때문에 사용자들이 제3자의 모니터링 아래에 놓일 수 있고 서로 다른 물건과 개인들 사이의 데이터 흐름을 통제하기 어렵기 때문에 애초 수집 목적 외 이용의 가능성이 클 뿐만 아니라 원소스의 데이터를 가공하여 다양한 목적에 활용할 수 있다고 우려했다[3].

이미 세계 각국은 새로운 기술과 서비스 개발에 필요한 개인정보의 안전한 활용을 촉진하면서도, 증가하는 개인정보 침해 위협에 대응하기 위한 법제의 개편을 시도하고 있다. 대표적인 것이 유럽연합의 GDPR이다. GDPR은 2012년에 제안되어 4년간의 논의를 거쳐 2016년 5월 24일 채택되었고 2018년 5월 25일 발효되었는데, 기술 발전으로 기존의 개인정보보호 디렉티브(95/46/EC)가 포함하지 못했던 새로운 규정들을 신설하여 개인정보 보호를 강화하고자 하였으며, 디지털 단일 시장(Digital Single Market)에 대한 유럽연합의 기본 계획에 따라 유럽연합 가입국 내 정보의 자유이전을 보장하고자 하였다[4]. GDPR은 삭제권(잊힐 권리), 처리제한권, 개인정보 이동권, 프로파일링 거부권 등 정보주체의 권리를 신설하였으며, 개인정보 영향평가, 설계 및 기본설정에 의한 개인정보 보호(Data Protection by Design and by Default), 독립 정보보호 책임자(DPO)의 지정, 처리활동의 기록 의무화 등 개인정보처리자의 책임성을 위한 조치를 강화하였다. 개인정보

3) ARTICLE 29 DATA PROTECTION WORKING PARTY(2014a), "Opinion 8/2014 on the on Recent Developments on the Internet of Things", 14/EN WP 223.
4) EDPS(2015), "Meeting the Challenges of Big Data: A call for transparency, user control, data protection by design and accountability Opinion".

감독기관의 독립성과 권한을 규정하고 유럽연합 차원에서 법 적용의 일관성을 위해 개인정보보호이사회(European Data Protection Board, EDPB)를 설립하였다. 규정 위반시 최대 전 세계 연간 매출액 4% 또는 2천만 유로 중 높은 금액을 과징금으로 부과할 수 있도록 하는 등 제재도 강화하였다.

유럽평의회가 1981년 채택한 <개인정보의 자동처리와 관련된 개인의 보호를 위한 유럽회의 협약>, 즉 108호 협약은 개인정보 보호를 위한 구속력 있는 유일한 국제협약[5]으로서 유럽평의회 회원국이 아닌 국가에게도 가입을 열어두고 있다. 유럽평의회는 2018년 5월 18일, 현대화된 108호 협약(Modernized CoE Convention 108)[6]을 채택하였는데, 이는 신기술의 발전에 따른 환경의 변화를 협약에 반영하기 위한 것이다. 현대화된 108호 협약(108+ 협약)은 ▲ 조약 가입국 국민은 국적에 상관없이 어디서나 보호받을 수 있도록 하였고, ▲ 유전정보, 생체인식정보, 노동조합 가입 여부, 민족 등 민감정보의 목록을 확대하였으며, ▲ 보안 침해사고시 지체 없이 통지하도록 하였고, ▲ 오로지 자동화된 처리에 기반한 결정에 종속되지 않을 권리 등을 신설하였다.

한국 정부 역시 2010년대 초반부터 빅데이터 등 신기술 발전에 대응하여 개인정보 보호 규범의 변화를 도모해왔다. 그러나 그 방향은 주로 빅데이터 산업 활성화를 명분으로 개인정보 보호를 완화하는 것에 맞추어졌다[7]. 2013년 9월 당시 안전행정부가 발표한 <공공정보 개방공유에 따른 개인정보 보호 지침>, 2014년 12월 행정자치부와 한국정보화진흥원이 발표한 <개인정보 비식별화에 대한 적정성 자율평가 안내서>, 2014년 12월 방송통신위원회가 만든 <빅데이터 개인정보보호 가이드라인> 등이 그것이다. 이렇게 각 정부부처마다 서로 다른 가이드라인이 만들어지자, 2016년 6월 박근혜 정부는 관계부처 합동(국무조정실, 행정자치부, 방송통신위원회, 금융위원 회, 미래창조과학부, 보건복지부)으로 <개인정보 비식별조치 가이드라인>을 발표하였다. 그러나 개인정보 보호법 상의 근거 없이 개인정보 보호를 완화하고자 하는 이러한 시도들은 시민사회의 반발을 불러일으켰고, 시민단체는 비식별 전문기관과 20개 기업이 개인정보를 동의없이 처리한 것에 대해 개

5) “The Convention is the first and only binding international legal instrument protecting data privacy”, <https://epic.org/privacy/intl/coeconvention/> 참조.
6) https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e 참조.
7) 빅데이터와 개인정보를 둘러싼 국내 논란에 주요 경과에 대해서는 이광석 외(2018), 4차 산업혁명 시대에서 정보인권 보호를 위한 실태조사, 국가인권위원회 연구용역 보고서, pp161-170 참조.

인정보 보호법 등 위반으로 검찰에 고발하기도 하였다.

문재인 정부는 ‘대통령직속 4차산업혁명위원회’를 설치하고 “4차 산업혁명 시대, 미래 산업의 원유가 바로 데이터”라고 강조하며 “데이터의 개방과 공유를 확대해 활용도를 높이는” 데이터 규제혁신의 목표를 표방하였다[8]. 4차산업혁명위원회는 사회적 논란이 있는 정책에 대한 사회적 합의 도출을 목적으로 ‘규제·제도혁신 해커톤’이라는 행사를 개최하였는데, 2018년 초에 두 차례에 걸쳐 ‘개인정보의 보호와 활용의 조화’ 의제도 다루어졌다. 이 행사를 통해 ’가명정보‘ 개념의 도입 등 개인정보 관련 법적 체계를 정비할 필요성에 대한 합의는 이루어졌으나, 가명정보의 활용 목적과 범위, 그리고 개인정보의 결합 이슈와 관련해서는 합의가 이루어지지 못했다. 정부는 2018년 12월, 개인정보 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 ’정보통신망법‘), 신용정보의 이용 및 보호에 관한 법률(이하 ’신용정보법‘) 등 소위 ’데이터 3법‘ 개정안을 여당 의원을 통해 발의하였고 2020년 1월 9일 국회를 통과하여 같은 해 8월 5일 시행되었다.

데이터 3법의 주요 내용은 크게 두 가지이다. 첫째는 정보주체의 동의 없이 과학적 연구, 통계작성, 공익적 기록보존 등의 목적으로 가명정보를 이용할 수 있는 근거를 마련하는 것, 둘째는 개인정보의 오용·남용 및 유출 등을 감독할 감독기구는 개인정보 보호위원회로, 관련 법률의 유사·중복 규정은 개인정보 보호법으로 일원화하는 방향으로 법제를 체계적으로 정비하는 것이다[9]. 그러나 시민사회는 ‘데이터 3법’을 크게 비판하였다.[10] 과학적 연구(scientific research)를 ‘과학적 방법을 사용하는 연구’로 정의하여 신상품 개발 등 기업 내부적으로 수행하는 연구로까지 그 범위를 확대하는 한편, 전문기관을 통해 두 기업의 고객정보 결합을 허용하고 가명정보 형태의 반출을 허용함으로써 사실상 상업적 목적의 개인정보 판매, 결합, 공유를 허용하였다는 것이다.

본 연구에서는 우리나라 개인정보 보호 법제의 개정 결과물에 대하여 세 법제의 정합

8) 대통령 비서실 발표자료, 2018.8.31., “데이터경제 활성화 규제혁신 현장방문 인사말”, <https://www1.president.go.kr/articles/4122>.
9) 개인정보 보호법 법률 제16930호 “개정이유”, <http://www.law.go.kr/lsInfoP.do?lsiSeq=213857&lsId=&efYd=20200805&chrClsCd=010202&urlMode=lsEfInfoR&viewCls=lsRvsDocInfoR&ancYnChk=0#> 참조.
10) 시민사회단체 기자회견, 2019.12.9., “개인정보 도둑법 강행하는 정부 규탄한다”, <http://act.jinbo.net/wp/41952/>.

성과 상호 모순점이 없는지, 국제규범 중 특히 GDPR과의 적정성은 충족하고 있는지, 충족하지 못하는 부분은 무엇인지, 이를 충족하기 위해서는 어떻게 개정되어야 하는지를 집중 검토한다. 개정 개인정보 보호법은 개인정보 보호 체계의 정비와 관련해서 개인정보 보호위원회를 중앙행정기관으로 격상하고 행정안전부 및 방송통신위원회의 개인정보 감독권한을 통합하기는 하였으나 신용정보법 및 금융위원회의 감독권한까지 통합하지는 못하였다. 더구나 개정된 신용정보법은 가명정보의 연구목적 제공 및 결합과 관련된 개념과 절차를 개인정보 보호법과 다르게 규정하여 법률간의 중복과 혼란을 해소한다는 입법 취지에 반한다는 비판도 제기되었다. 또 가명정보의 동의없는 활용을 허용하면서도, 프로파일링 등 자동화된 처리에 대한 정보주체의 거부권, 설계 및 기본설정에 의한 개인정보 보호 등 신기술 환경에서 정보주체의 권리를 보호하고 개인정보처리자의 책임성을 강화하는 규정은 포함되지 않았다. GDPR이 2012년에 초안이 제안되어 4년 동안의 논의를 거쳐 2016년 5월 채택된 것에 비해, 한국의 개인정보 보호법은 개정 과정에서 사회적인 갈등만을 드러냈을 뿐 시대적인 변화를 수용하기에는 미흡했다는 점에서 지금이라도 개인정보 보호 법제에 대한 제대로 된 평가와 개선이 필요할 것이다.

2020년 8월 5일 출범한 통합 개인정보 보호위원회는 여러 과제를 떠안게 되겠지만, 개인정보 보호법의 전반적인 개정 역시 중요한 과제 중의 하나가 될 것으로 보인다. 그 이유는 우선 현재의 개인정보 보호법이 정보통신망법과 통합하는 과정에서 정보통신망법의 규정을 ‘특례’ 형태로 형식적으로만 통합하였기 때문이다. 즉, 통합은 되었지만 중복·유사 규정으로 인한 혼란은 여전히 남아있는 바, 빠른 시일 내에 이를 정비할 필요가 있다. 둘째, 개인정보 보호법 개정 과정에서 정보통신망법을 통합하고 행정안전부와 방송통신위원회의 감독 권한을 개인정보 보호위원회로 이관하기는 했지만, 여전히 신용정보법과는 중복·유사 조항이 남아있으며 금융위원회의 감독권한도 그대로 유지되었다. 특히 과학적 연구 목적 활용과 데이터 연계 등 쟁점이 되었던 사안에 대해 개인정보 보호법과 신용정보법이 다른 태도를 취하고 있고 실제 이행 과정에서 개인정보 보호위원회와 금융위원회의 입장 차이가 발생할 경우 더욱 혼란이 심화될 우려도 있다. 혼란을 최소화할 수 있는 방향으로 두 법률 모두 정비가 이루어질 필요가 있다. 셋째, 우리나라도 다른 나라와 마찬가지로 신기술 환경에 대응하여 정보주체를 보호하기 위해 요구되는 새로운 권리와 개인정보처리자의 책임성을 강화하기 위한 규정을 반영할 필요가 있다. 프로

파일링에 대한 정보주체의 권리, 개인정보 이동권, 개인정보 영향평가의 실질화, 설계 및 기본설정에 의한 개인정보 보호, 독립적인 정보보호 책임자(DPO) 제도 등이 주된 쟁점이 될 것으로 보인다.

이와 같은 개인정보 보호법의 개선방안을 모색하는 과정에서 관련 국제규범을 고려할 필요가 있다. 개인정보의 국가간 이동이 증가하고 있는 현실을 고려할 때 각 국가의 개인정보 보호 수준이 동등하게 유지되어야 개인정보가 어디서나 적절하게 보호될 수 있을 것이다. 개인정보처리자 입장에서도 국가간 통일성이 유지되어야 기업 내부의 개인정보 보호 체계 구축을 위한 법률적, 행정적 비용을 줄일 수 있을 것이다.

현재 개인정보 보호 관련 국제규범에 가장 가까운 것은 108+ 협약이다. 이 협약은 유럽평의회 비회원국도 가입할 수 있도록 열려있다. 2019년 7월 한국을 방문했던 조셉 카나타치 유엔 프라이버시 특별보고관은 한국 개인정보 보호위원회의 독립성을 강화할 필요성을 언급하며 이 '국제 표준 협약'(international standard-setting convention)에 한국도 가입할 것을 강하게 권고했다[11]. GDPR은 108+ 협약과 양립 가능하며 유럽이사회(European Council)도 2019년 4월 9일, 유럽연합 회원국이 108+ 협약을 비준할 것을 결정하였다[12].

GDPR 역시 유럽연합 차원의 개인정보 보호법이지만 사실상 국제규범의 위상을 가지고 있다. GDPR의 적용 범위는 비단 유럽연합 역내에 설립된 개인정보처리자로 한정되지 않으며 유럽연합 시민의 개인정보를 처리하는 모든 처리자로 확대된다. 또한 GDPR은 개인정보의 국가간 이동을 위한 조건의 하나로 다른 나라가 유럽연합에 상응하는 개인정보 보호수준을 가지고 있는지 평가하는 '적정성 평가' 제도를 가지고 있다. 한국 정부가 개인정보 보호법 개정을 통해 개인정보 보호위원회의 독립성과 권한을 강화한 이유 중 하나도 유럽연합의 적정성 결정을 통과하기 위한 것이었다. 이처럼 GDPR 적정성 결정은 GDPR을 국제규범화하는 하나의 계기가 되고 있다.

---

11) Joseph CANNATACI UN Special Rapporteur on the Right to Privacy, 2019.7.26., "Statement to the media by the United Nations Special Rapporteur on the right to privacy, on the conclusion of his official visit to the Republic of Korea", <https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=24860&LangID=E>.

12) "Convention 108+", <https://edri.org/protecting-personal-data-world-wide-convention-108/>.

본 연구는 빅데이터와 인공지능 등 신기술 환경에서 개인정보 자기결정권을 보호하기 위한 국내 법제도 개선방안의 도출을 목적으로 한다. GDPR, 108+ 협약, OECD 및 유엔 가이드라인 등 개인정보 보호 국제규범에 대한 면밀한 검토와 국내 법제와의 비교 분석을 통해 국내 법제에서 도입이 필요한 이슈들을 도출하고 국내 환경에서 어떻게 도입하면 좋을지 적절한 방안을 권고하고자 한다.

또한 본 연구는 최근 개정된 개인정보 보호를 위한 세 법제가 정합성을 갖추고 있는지, 상호 모순점은 없는지를 검토한다. 첫째, 과거부터 제기되어 오던 세 법제의 상호 모순점이 해소되었는지를 검토한다. 예를 들어 적용 범위 판단의 곤란, 감독기관 상호간의 관계, 시행령과 고시 등의 제정권, 세 법제의 보호 수준의 상이함 등을 들 수 있다. 둘째, 개정된 세 법제로 인해서 새롭게 부각되는 상호 모순점은 무엇인지를 검토한다.

본 연구는 전술한 것처럼 우리나라 개인정보 보호 법제가 국제규범과의 조화, 특히 GDPR과의 적정성을 갖추고 있는지를 검토, 평가한다. 아울러 이를 충족하기 위해서 필요한 개정사항을 도출한다. 개인정보 감독기관의 독립성, 국가 감시와 적법절차 준수 여부에 대한 평가, 자동화된 결정에서의 개인정보 자기결정권의 보호 등을 포함한다.

더 나아가 빅데이터와 인공지능 등 신기술 환경에서 개인정보 자기결정권을 보호하기 위한 국내 법제도 개선방안도 검토한다. 이와 관련해서는 국제규범과의 조화와 GDPR을 포함한 해외 법제와의 비교 검토를 통해서 개선방안을 도출한다. GDPR의 다양한 제도와 국내 법제를 비교하고, 특히 신용정보법에서 도입한 제도들을 해외 법제와 비교 평가할 것이다. 이미 GDPR의 채택 및 발효를 전후해서 국내에서도 GDPR 주요 이슈에 대한 소개가 이루어졌으며, 정부도 국내 기업들을 위한 GDPR 안내서를 발간한 바 있다. 또한 지능정보사회 혹은 4차 산업혁명 시대에 적합한 개인정보 보호 체계의 개선방안에 대한 연구가 이루어져 왔다. 이러한 기존 논의를 토대로 하되, 2020년 초 데이터 3법이 통과한 국내 상황의 변화, 그리고 EDPB의 GDPR에 대한 최근 가이드라인 및 유럽사법재판소(ECJ)의 개인정보 관련 판결 등 최근 동향을 반영하여 국내 개인정보 보호 법제 개선을 위한 의제들을 종합적으로 정리해보고자 한다.

한편, 개인정보 보호위원회와 국가인권위원회 사이의 역할 정립도 필요하다. 특히 인공지능이 인권에 미치는 영향은 비단 개인정보 문제에 국한하지 않고 표현의 자유, 차별 등 인권 전반에 폭넓게 미치는 만큼 국가인권위원회가 해야 할 역할이 크다. 국제 개인

정보 보호 감독기관 협의회(ICDPPC)는 인공지능 문제에서 “개인정보 감독기관들과 인권 기구들의 협력”이 필요하다고 강조한 바 있다[13]. 이와 관련하여 개인정보 감독기관(DPAs)과 국가인권기구(NHRIs)의 역할 정립과 상호작용, 두 기구의 구성 원리와 기능 및 목적의 차이[14], 개인정보 보호 및 인권 전반에 대한 보호의 상호작용 등을 검토, 평가하고, 우리나라의 국가인권기구가 해 온 역할 및 해외 사례를 검토, 평가해 본다.

해외 국가인권기구들은 최근 인공지능 등 신기술로 인한 인권침해 이슈에 적극적으로 개입하고 있다. 일례로 유럽연합 기본권청(European Union Agency for Fundamental Rights, 이하 FRA)의 데이터 보호, 개인정보 및 새로운 기술에 대한 적극적인 의견제시를 들 수 있다. FRA는 유럽연합 회원국의 인공지능 정책에 대한 배경 연구로서 AI 정책 이니셔티브(2016-2019), 2019년의 <얼굴 인식 기술 : 법 집행 상황에서 기본적인 권리 고려 사항> 등을 비롯하여 활발한 의견제시를 해 오고 있다. 호주 국가인권위원회는 <인권과 기술(Human Rights and Technology) 프로젝트>를 발족한 바 있다. 한편, 한국 정부는 2019년 12월, <AI 국가전략>을 발표하였다[15]. “IT 강국을 넘어 AI 강국으로”라는 비전에서 보여지듯이 자칫하면 산업육성이라는 관점에 치우쳐 인공지능에 대한 개입이 이루어질 우려도 있다. ‘사람 중심 AI’라는 목표가 부작용에 대한 대응을 넘어 AI 개발과 도입의 방향 설정까지 아우르기 위해서는 개인정보 보호위원회와 국가인권위원회의 적극적인 개입이 필요하다.

제2절 연구내용 및 범위

본 연구는 우선 제2장 및 제3장에서 개인정보 보호와 관련된 국내외 현황을 살펴보고, 제4장부터 제7장에 걸쳐 국내 개인정보 보호 규범의 개선 방향을 제시하였다.

제2장에서는 빅데이터, 인공지능 등 신기술의 발전에 대응하여 최근 몇 년 동안 세계 개인정보 규범이 어떻게 변화하였는지를 중심으로 살펴보았다. 2013년 개정된 OECD 가

13) ICDPPC(2018), “Declaration on Ethics and Data Protection in Artificial Intelligence”.
14) European Union Agency for Fundamental Rights(FRA)(2010a), “National Human Rights Institutions in the EU Member States, Strengthening the fundamental rights architecture in the EU I”.
15) 정책브리핑, 2019.12.17, “AI 국가전략 발표…2030년 455조 창출.AI반도체 세계 1위”, <http://www.korea.kr/news/policyNewsView.do?newsId=148867621>.

이드라인, 정보기관의 인터넷 대량감시 폭로 이후 유엔에서 채택된 <디지털 시대 프라이버시권 결의안>, 유럽평의회의 108호 협약 현대화 등 최근 국제규범의 동향을 다루었다. 이어 유럽, 미국, 일본의 개인정보 보호 법제 동향을 간략하게 정리하였다. 유럽연합의 GDPR은 기존 개인정보보호 디렉티브와 어떻게 달라졌는지 간략하게 살펴본 후, GDPR 시행 2년 평가를 자세하게 다루었다. 이는 GDPR이 사실상 전 세계 개인정보 보호 법제의 모델이 되고 있음을 고려할 때, GDPR이 실제 현실에 어떠한 영향을 미치고 있고 개선점은 무엇인지에 대한 평가가 중요하기 때문이다. 이어 사실상 유럽연합의 규범 형성에 중대한 영향을 미치고 있는 유럽사법재판소의 개인정보 관련 최근 판결에 대해 소개하였다.

제3장에서는 국내 개인정보 보호 법제를 둘러싼 최근 과제를 다루었다. 2020년 1월에 소위 '데이터 3법'이 국회를 통과함으로써 최근 몇 년 동안 이어진, 빅데이터와 개인정보를 둘러싼 사회적인 논란이 일단락되었다. 데이터 3법을 둘러싼 논란이 무엇이었고, 데이터 3법 통과로 인해 해결이 된 문제는 무엇이고 새롭게 제기된 문제는 무엇인지, 어떠한 문제가 여전히 남아있는지 정리함으로써 향후 개인정보 보호 법제를 어떻게 개선해야 하는지 큰 방향을 제시하고자 하였다.

이와 같은 국내외 현황 분석과 개선 방향을 토대로, 제4장부터는 중요한 이슈별로 구체적인 개선방안을 검토하였다. 개선방안은 크게 정보주체의 권리보호 강화 방안(제4장), 개인정보처리자의 책임성 강화 방안(제5장), 범죄예방 및 수사 등 분야에서 개인정보 보호 방안(제6장)으로 구분하였다.

제4장에서는 열람권 등 기존 정보주체의 권리들을 GDPR 및 미국 캘리포니아 소비자 프라이버시 보호법(CCPA) 등의 내용과 비교하면서 개선방안을 제시하였고, 현재 국내 개인정보 보호법에는 없는 새로운 권리로서 개인정보 이동권 및 프로파일링을 포함한 자동화된 의사결정과 관련된 정보주체의 권리를 상세하게 분석하였다. 이는 인공지능 시대에 반드시 도입이 필요한 권리일 것이다. 또한 국내에서도 실효성 논란이 제기되고 있는 동의 제도가 어떻게 개선되어야 하는지 살펴보았다.

제5장에서는 해외 규범을 참고하여 개인정보처리자의 책임성을 강화하기 위한 다양한 제도를 분석하였다. 개인정보 영향평가와 같이 이미 국내에 도입되어 있지만 좀 더 확대·강화할 필요가 있는 제도도 있고, 설계 및 기본설정에 의한 개인정보 보호와 같이 새롭

게 도입할 필요가 있는 제도도 있다. 국내에 이미 개인정보 보호책임자 제도가 있기는 하지만, 독립적인 정보보호 책임자(DPO)는 그 역할과 성격이 다르기 때문에, DPO 제도 역시 도입을 검토할 필요가 있다.

제6장은 범죄예방과 수사 등 분야에서 개인정보 보호 이슈를 다루었는데, 이는 이 분야가 일반적인 개인정보 보호 규범의 적용이 배제되는 예외로 취급되어 개인정보 보호의 사각지대로 남아있기 때문이다. 그러나 일반적인 개인정보 보호 규범이 동일하게 적용되지는 않더라도 개인정보 남용을 막을 수 있는 법제 및 감독 메커니즘은 필요하다. 이에 유럽연합의 경찰 디렉티브의 주요 내용을 검토하고 국내 법제의 개선방안에 대해 제안하였다.

개인정보의 보호에 대한 감독은 주로 개인정보 감독기관인 개인정보 보호위원회의 역할로 여겨진다. 그러나 개인정보 자기결정권 및 프라이버시권이 중요한 기본권의 하나임을 고려할 때 국가인권위원회의 역할 역시 중요하다. 특히 인공지능이 인권에 미치는 영향은 개인정보 및 프라이버시권에 한정되지 않는다. 개인정보 보호위원회와 국가인권위원회가 개인정보 및 프라이버시권 보호를 위해 어떠한 역할을 담당하고, 혹은 상호 협력할 것인지에 대해 아직 국제적으로 확립된 규범이 있는 것은 아니다. 제7장에서는 개인정보 보호 분야에서 국가인권기구와 개인정보 감독기관의 역할을 분석하고, 상호 역할 분담 및 협력하는 국내외 사례를 검토하면서 향후 국가인권기구가 해야 할 역할을 제안하였다.

마지막 제8장에서는 연구의 결론과 함께, 향후 구체적인 정책 및 입법이 되어야 할 사항들을 정책권고로 제안하였다.

제2장 신기술 발전과 세계 개인정보 보호 규범의 변화

각국의 개인정보 보호 법제의 형성에 지대한 영향을 미친 최초의 국제 규범으로 1980년에 경제협력개발기구(OECD)가 작성한 「프라이버시 보호와 개인정보의 국제유통에 대한 가이드라인(이하 OECD 프라이버시 가이드라인)」도 자동화된 개인정보 처리의 발전과 방대한 개인정보들의 국경을 넘는 유통을 배경으로 한다. 그러나 이후에도 빅데이터, 사물인터넷, 인공지능 등 신기술이 급속하게 발전하고 있으며, 이에 따라 개인정보를 수집, 처리하는 방식도 계속 달라지고 있다. 또한 인터넷과 모바일 기기의 확산으로 구글, 페이스북 등 전 세계 이용자를 대상으로 서비스를 제공하는 거대 IT 기업을 필두로 상품과 서비스의 세계적인 유통이 활성화되면서 국경을 넘는 개인정보 수집, 처리 역시 보편화되고 있다. 개인정보 보호 규범도 이러한 기술·사회·경제적 환경의 변화에 대응하여 발전하고 있으며, 각국의 서로 다른 규범이 통일화되는 경향도 강화되고 있다. 2010년 이후, OECD, 유럽평의회(Council of Europe), 유럽연합 등 국제적인 수준에서 개인정보 보호 체제가 새로운 기술 환경에 맞게 업데이트되었다. 이 장에서는 유엔 등 국제기구 및 세계 주요 국가에서 최근 개인정보 보호 규범이 어떻게 변화해 왔는지 간략히 검토해보고자 한다.

제1절 유엔 등 국제기구의 개인정보 보호 규범

1. 경제협력개발기구(OECD)

1980년 가이드라인은 기술중립적으로 작성되어 그동안의 기술적, 사회적 변화에도 불구하고 30여 년간 유지되어 왔지만, 개인정보 활용 및 보호 방식의 변화에 따라 결국 업데이트될 필요성에 직면하였다. 2008년 <인터넷 경제의 미래를 위한 서울 선언>은 “변화하는 기술, 시장, 이용자의 행동, 중요성이 커지고 있는 디지털 정체성”에 비추어 1980년 가이드라인을 포함한 OECD의 일부 문서를 검토할 것을 권고했으며, 가이드라인 채택 30주년이 되는 2010년에 평가를 위한 준비 작업이 시작되었다. ‘정보 보안 및 프라이버시 작업반(Working Party for Information Security and Privacy, WPISP)은 다양한 이해당사자들로 구성된 전문가 그룹의 지원을 받아 수정된 가이드라인을 만들었으며, 이

는 2013년 7월 11일 채택되었다[16].

수집 제한의 원칙(Collection Limitation Principle), 정보 정확성 원칙(Data Quality Principle), 목적 명시의 원칙(Purpose Specification Principle), 이용 제한의 원칙(Use Limitation Principle), 안전성 확보의 원칙(Security Safeguard Principle), 공개의 원칙(Openness Principle), 개인 참가의 원칙(Individual Participation Principle), 책임의 원칙(Accountability Principle) 등 1980년 가이드라인의 <개인정보 보호 8원칙>은 2013년 가이드라인에도 그대로 포함되었다. 그러나 기존 가이드라인에서 두 가지 측면을 고려하여 증보되었는데, 첫째는 위험 관리에 기반한 접근을 통한 프라이버시 보호의 실질적인 이행, 둘째는 상호운용성 증진을 통한 국제적인 차원의 프라이버시 대응 노력의 필요성이다. 이는 현대적인 개인정보 보호의 특징점을 반영하고 있는데, 위험 관리를 기반으로 한 프라이버시 보호라는 관점은 국가별로 형식적 차원의 개인정보 보호 규범들이 증가하고 있는 상황에서, 그러한 형성적 규제체계가 실질적인 프라이버시의 침해 위험을 방지하지 못하면서도 국제적 교류 및 거래에 장애물로 등장하고 있는 상황을 염두에 둔 것이며, 국제적 차원에서의 규범간 상호운용성 증진은 급증하고 있는 국경간 개인정보 이동 문제에 직면하여 개인정보 보호의 실질적인 규범력을 증진시키기 위한 노력이라고 할 수 있다[17].

2013년 가이드라인은 국가 프라이버시 전략(National privacy strategies), 프라이버시 관리 프로그램(Privacy management programmes), 개인정보 유출 통지(Data security breach notification) 등 새로운 개념도 도입하고 있다. 3부 '책무성 이행(IMPLEMENTING ACCOUNTABILITY)'은 2013년 가이드라인에 새롭게 추가되었는데, 책무성 이행을 위한 개인정보처리자의 의무를 규정하고 있다. 예를 들어, 개인정보처리자는 프라이버시 관리 프로그램을 두고, 프라이버시 위험 평가에 기반한 적절한 안전조치를 제공해야 한다(15조 a. iii.). 또한 중대한 보안 침해 사고가 발생했을 경우 프라이버시 집행 당국(개인정보 감독기관) 및 정보주체에게 고지해야 한다(15조 c.). 국가는 이 가이드라인을 이해하기 위해, 국가 프라이버시 전략을 개발해야 하며(19조 a.), 거버넌스와 자원, 기술적 역량을 가진 프라이버시 집행 당국을 설립, 유지해야 한다(19조 c.).

16) OECD(2013), "The OECD Privacy Framework".
17) 이은우 외(2018), EU GDPR 등 개인정보보호 규범 및 감독기구의 국제표준 확립 필요성 연구 - 국제규범의 변화와 국내 개인정보 보호체계 효율화 방안 연구, p6.

2. 유엔

유엔 인권 규범에 개인정보의 보호가 명시적으로 규정되어 있는 것은 아니다. 그러나 1948년 세계인권선언 제12조, 1976년에 발효된 시민적, 정치적 권리에 관한 국제규약(ICCPR) 제17조에서 자신의 프라이버시, 가족, 주택, 통신에 대해 함부로 침해받지 않을 권리를 규정하고 있다. 개인정보의 보호와 관련해서는 1990년 12월 14일, 총회에서 <컴퓨터화된 개인정보 파일의 규제를 위한 가이드라인> 결의안을 채택한 바 있다[18].

그러나 2013년 에드워드 스노든이 미국 국가안보국(NSA)등 정보기관에 의한 인터넷 대량감시를 폭로한 이후, 유엔은 거의 매년 총회 및 인권이사회(Human Rights Council)의 결의안을 통해 디지털 시대 프라이버시 보호를 위한 적절한 조치를 취할 것을 각국 정부에 촉구하고 있다. 스노든의 폭로가 있었던 2013년 12월에 열린 유엔 총회에서는 통신감시와 관련된 절차와 관행, 법률을 재검토할 것과 독립적이고 효율적인 감독체계 등 국가 감시를 통제하는 조치를 각국 정부에 권고하는 <디지털 시대 프라이버시권 결의안>[19]이 채택되었다. 결의안의 요청에 따라 2014년 <디지털 시대 프라이버시권 보고서>[20]를 발간한 유엔 인권최고대표는 디지털 시대 커뮤니케이션 기술은 정부, 기업, 개인이 감시, 도청, 개인정보 수집을 실행할 수 있는 능력 또한 향상시켜 왔다고 우려하였다.

유엔 총회 디지털 시대 프라이버시권 결의안(2013년 12월 18일)

4. 모든 국가들에 다음을 요청한다.
(a) 디지털 통신의 맥락에서 프라이버시권을 존중하고 보호할 것
(b) 관련 국내법이 국제인권법상 의무를 준수하도록 하는 등, 권리 침해를 종식시키고 그 침해를 방지하는 조건을 창출하기 위한 조치를 취할 것
(c) 국제인권법상 모든 의무를 완전하고 효율적으로 이행함으로써 프라이버시권을 보장하기 위한 목적에서, 대량 감시, 감청 및 수집을 비롯한 각국 통신감시, 감청, 개인정보 수집과 관련한 절차와 관행, 법률을 재검토할 것.
(d) 국가의 통신 감시, 감청 및 개인정보 수집에 대해 적절한 투명성과 책임성을 보장하는 독립적이고 효율적인 국내 감독 체계를 설립하거나 운영할 것

18) UN(1990), Guidelines for the Regulation of Computerized Personal Data Files, Adopted by General Assembly resolution 45/95 of 14 December 1990.
19) UN(2014), The right to privacy in the digital age, A/RES/68/167. Resolution adopted by the General Assembly on 18 December 2013, 2014.1.21.
20) OHCHR(2014), The Right to Privacy in the Digital Age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37. 2014.6.30

이제 국가는 동시적, 침투적, 표적적이거나 광범위한 감시를 수행할 수 있는 능력을 그 어느 때보다 막대하게 보유하게 되었으며, 지구적 정치, 경제, 사회가 깊이 의존하고 있는 기술 플랫폼은 대량감시에 취약할 뿐 아니라 이를 촉진하는 환경이다. 반면 많은 국가에서 프라이버시 보호를 위한 입법과 집행이 제대로 이루어지지 않고 있고 무엇보다 감독이 효과가 없었다는 점에 대해 우려를 나타냈다. 이에 유엔 인권최고대표는 국제 인권법에 반하는 전자감시 정책 및 수단들에 대한 모든 평가는 변화하는 문제의 속성을 고려해서 반드시 다듬어져야 한다는 점, 그리고 효과적이고 독립적인 감독을 위한 조치들이 취해져야 함을 권고했다.

유엔 총회는 2015년[21]과 2017년[22]에도 <디지털 시대의 프라이버시권에 대한 결의안>을 채택하면서 프라이버시권 등 오프라인에서 사람들이 가진 것과 동일한 권리가 온라인에서도 보호되어야 한다고 선언하였다. 유엔의 결의안들이 정보기관의 감시에 대한 폭로를 계기로 하여 채택이 되었고 주로 국가의 대량감시에 대한 비판과 정보기관 권한의 제한 필요성에 초점을 맞추고 있기는 하지만, 2017년 결의안에서는 개인정보 처리와 관련된 기업의 증가하는 역량이 디지털 시대 프라이버시권에 위험을 야기할 수 있음을 명확하게 언급하고 있다[23]. 2017년 결의안은 국가뿐 아니라 기업이 자의적이고 불법적인 방식으로 프라이버시권에 간섭하는 것에 대하여 통제하는 조치를 취하고, 시민들의 디지털 리터러시와 기술 역량을 함양하기 위해 교육 기회를 장려할 것을 각국에 촉구하였다. 개인의 자유롭고, 명시적이고, 충분한 설명에 따른 동의 없이 개인정보가 판매되고 다목적으로 재판매되며 타 기업에 공유되는 피해에 대하여 우려를 표하고, 이에 대한 규제, 예방 조치 및 구제대책을 취할 것을 각국에 요구하기도 하였다[24].

2015년 3월 26일, 유엔 인권이사회는 디지털 시대 프라이버시권에 대한 체계적인 대응을 위해 프라이버시 특별보고관을 신설하였으며, 조셉 카나타치를 첫번째 특별보고관으로 임명하였다. 그는 2019년 7월, 실태조사를 위해 한국을 공식 방문하기도 하였다.

---

21) UN(2015), The right to privacy in the digital age, Resolution adopted by the General Assembly on 18 December 2014, A/RES/69/166. 2015.1.10

22) UN(2017), The right to privacy in the digital age, Resolution adopted by the General Assembly on 19 December 2016, A/RES/71/199. 2017.1.25

23) European Union Agency for Fundamental Rights(FRA)(2018a), Handbook on European data protection law – 2018 edition, 2018.5.25. p21-22.

24) 이광석 외(2018), 4차 산업혁명 시대에서 정보인권 보호를 위한 실태조사, 2018년도 인권상황실태조사 연구용역보고서, pp141-142.

3. 유럽평의회

유럽평의회(Council of Europe)는 2차 세계대전 이후에 유럽 국가들의 법치, 민주주의, 인권, 사회 발전을 증진하기 위해 만들어졌다. 이를 위해 1950년에 유럽인권조약[25]을 채택하였는데, 이는 회원국에 조약 준수의 의무를 부여한다. 이를 보장하기 위해 1959년 프랑스 스트라스부르에 유럽인권재판소가 설립되었다. 유럽인권조약 제8조는 사생활, 가정생활, 주택, 통신을 존중받을 권리를 가지고 있음을 선언하며, 그러한 권리 제한이 허용될 수 있는 조건을 설정하고 있다[26].

1981년에 유럽평의회가 체결한 <개인정보의 자동화된 처리에 관한 개인의 보호를 위한 협약>(일명 108호 협약이라고 부른다)[27]은 개인정보 분야에서 유일하게 법적으로 구속력 있는 국제협약으로 남아있다. 2001년에는 108호 협약의 추가 의정서[28]가 채택이 되었는데, 비회원국인 제3국으로의 개인정보 이전 문제, 국가 개인정보 감독기관의 의무적 설립 문제를 다루고 있다. 추가 의정서의 규정들은 이후 108호 현대화 협약으로 흡수되었다. 2008년 10월 스트라스부르에서 열린 30차 개인정보 감독기관 국제회의(The International Conference of Data Protection and Privacy Commissioners, ICDPPC)[29]에서는 유럽평의회 회원국 이외의 국가에 대해서도 108호 협약의 가입을 권장하기로 하고, 동 협약을 통해 각국 개인정보 감독기관의 협력을 촉진하는 결의안을 채택하였다. 이에 따라 비유럽 국가로서 처음으로 2013년 10월 우루과이가 108호 협약에 비준하였다. 108호 협약은 회원국들에게 협약의 개인정보 보호 규정을 국내법에 반영할 것을 의무화하고 있다. 다만, 구체적인 도입방법은 각국의 헌법이나 법제도에 따라 달라질 수 있다[30].

2011년부터 108호 협약의 현대화 작업이 논의되기 시작하였다. 108호 협약의 현대화는

---

25) Council of Europe, European Convention on Human Rights, CETS No. 005, 1950.
26) FRA(2018a) pp22-23.
27) Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981.
28) Council of Europe, Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows, CETS No. 181, 2001.
29) 2019년 10월에 ICDPPC는 글로벌 프라이버시 총회(Global Privacy Assembly)로 이름을 변경하였다.
30) 박훤일(2015), 유럽회의 108호협약의 의의와 우리나라 가입의 필요성, 경희법학 제50권 제4호, pp182-183.

크게 두 가지 목표를 가지고 있었다. 첫째는 새로운 정보통신기술의 활용에 따른 문제들에 대응하는 것이다. 둘째는 협약의 효과적인 이행을 강화하는 것이다. 또한 서로 다른 지역에서 발전해온 다양한 규범 체계를 모아서, 유연하고 투명하며 견고한, 그리고 효과적인 안전조치를 제공하면서도 국경간 개인정보 이전을 촉진할 수 있는 다자간 체제를 제안하기 위한 목적도 있다. 108호 현대화 협약은 ▲ 협약의 조항들은 원칙적인 수준에서 규정하고 보다 구체적인 규정들은 가이드라인이나 권고로 보완하고자 하였고, ▲ 유럽연합의 개인정보 보호 법제를 포함하여 다른 법제와의 일관성 및 호환성을 목표로 하였으며, ▲기술 중립적인 관점을 유지하고, ▲ 보편적 표준으로서의 협약의 잠재력을 재확인하고자 하였다. 2018년 5월 18일 각료이사회는 수정된 협약안(Protocol CETS No. 223)을 채택하였으며, 그 해 10월 10일부터 서명에 들어갔다[31]. 108호 협약의 현대화 작업은 2012년에 시작된 유럽연합의 개인정보 보호 규범의 개혁과 동시에 이루어졌으며, 유럽평의회와 유럽연합 당국들은 양자 사이의 일관성과 호환성을 보장하기 위해 노력하였다.[32]

108호 현대화 협약이 기존의 협약과 달라진 점은 다음과 같다[33].

○ 기존 협약은 '자동화된 개인정보 파일(automated data file)'을 대상으로 하였으나 새 협약에서는 파일 개념이 없어졌다. '개인정보 파일 컨트롤러(controller of a data file)'도 '개인정보 컨트롤러(data controller)'로 변경되었고, 프로세서와 수령자(recipient) 개념이 신설되었다. 기존 협약은 '자동화된 처리'를 대상으로 하였으나 새 협약은 자동화 여부와 무관하게 모든 형태의 개인정보 처리를 대상으로 한다. 또한 기존 협약은 회원국이 특정 분야(예를 들어 국가안보 분야)의 개인정보 파일에는 협약을 적용하지 않도록 사전에 선언하도록 했지만, 새 협약은 그러한 적용 예외 조항을 삭제하였다(2조).

○ 회원국은 협약이 효력을 가질 수 있도록 국내법에 필요한 조치를 도입해야 할 뿐만 아니라, 그러한 조치가 취해졌음을 입증해야 하고 협약 위원회(the Convention Committee)는 각국의 이행상황을 평가할 수 있다. ("follow-up mechanism" 이라 부른다)

---

31) Council of Europe, 2020.9.12., Modernisation of the Data Protection "Convention 108" <https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet>
32) FRA(2018a) p26.
33) Council of Europe. The modernised Convention 108: novelties in a nutshell

(4조) 또한 국제기구도 협약에 가입할 수 있도록 허용하였다(27조).

○ 개인정보 처리 과정 전반에 걸친 비례성 원칙(the principle of proportionality)을 강조하고 있으며 동의 및 다른 적법 근거 등 개인정보 처리의 법적 근거를 명확히 규정하였다(5조).

○ 민감정보(6조)에 유전자 정보, 생체인식 정보, 범죄 및 형사절차 관련 정보, 노동조합 가입 여부, 민족적 기원 등을 추가하였다.

○ 침해 사고가 발생할 경우 지체 없이 고지하도록 하였다(7조). 다만, 정보주체의 권리와 자유를 심각하게 침해할 경우로 제한되며, 최소한 감독기관에게는 고지되어야 한다.

○ 개인정보 처리의 투명성(8조)을 위해, 컨트롤러의 신원, 거주지, 처리 목적 및 처리의 적법 근거 등 컨트롤러가 정보주체에게 알려야 할 사항들을 규정하였다.

○ 디지털 시대에 적합한 정보주체의 권리를 규정하였다(9조). 정보주체가 열람을 요구할 수 있는 개인정보의 목록을 확대하고, 개인정보 처리의 결과가 자신에게 적용될 때 그 처리의 기반이 되는 논리(reasoning)를 요구할 권리를 보장하였다. 이는 프로파일링 맥락에서 특히 중요하며, 정보주체의 견해가 고려되지 않고 순전히 자동화된 처리에 기반한 결정에 종속되지 않을 권리의 보장과 연결된다. 컨트롤러가 자신의 정당한 이익이 우월하다는 것을 입증하지 못한다면, 정보주체는 언제든 자신의 개인정보처리에 반대할 권리를 갖는다.

○ 현대화 협약은 컨트롤러 및 프로세서에게 광범한 의무를 부과하고 있는데(10조), 컨트롤러가 개인정보 보호 규범의 준수를 입증하도록 하는 책무성이 핵심 요소이다. 컨트롤러는 설계 및 기본설정에 의한 프라이버시 보호, 개인정보 영향평가 등 개인정보 보호를 보장할 수 있는 적절한 모든 조치를 취해야 한다.

○ 이 협약의 권리를 법에 근거하여 제한할 수 있는데, 그 근거에 “공공 이익의 필수적인 목적” 및 표현의 자유가 추가되었다. 국가안보 및 방위 목적으로 위원회와 감독기관의 감독 권한이 일정하게 제한될 수 있지만, 그러한 목적의 개인정보 처리도 독립적이고 효과적인 평가 및 감독을 받아야 함을 명시하고 있다(11조).

○ 회원국 사이의 개인정보 이전은, 그러한 이전이 협약을 우회할 수 있는 실질적이고 심각한 위험을 야기할 경우 외에는 제한이 없다. 그러나 협약의 당사국이 아닌 국가로 이전할 경우에는 적절한 수준의 보호가 보장되어야 하는데, 이는 ▲ 법에 의해서 혹은

▲ 법적 구속력이 있고 집행 가능한, 승인된 표준적 안전조치(계약 조항 혹은 구속력 있는 기업 규칙)에 의해 가능하다(14조).

○ 2001년 108호 추가 의정서에 기반하여, 새 협약은 감독기관의 권한 목록을 보완하였다. 개입권, 조사권, 사법 절차를 개시할 권한 혹은 사법기관에 제소할 권한 등에 더하여 인식 제고, 정보 제공, 이해당사자 교육의 의무, 그리고 결정권(take decisions) 및 제재권(impose sanctions)도 부여하였다. 또한 업무와 권한에 있어 독립적이어야 함을 재천명하였다(15조).

○ 회원국 감독기관 사이의 협력 문제도 규정하였다(17조). 조사의 조정, 공동 활동의 수행, 법률 및 행정 관행에 대한 상호 정보 및 문서 제공 등을 해야 하며, 협력 강화를 위한 포럼을 신설하였다.

○ 기존 협약의 협의 위원회(Consultative Committee)를 새 협약에서는 권한이 강화된 협약 위원회(Convention Committee)로 대체하였다(22-24조). 협약 위원회는 협약의 해석, 정보의 교환, 개인정보 보호 표준 개발에 핵심적인 역할을 한다. 더이상 협의적 지위가 아니라 평가 및 감독 권한을 갖게 되었는데, 협약 가입 전에 개인정보 보호 수준에 대한 의견을 제시하고, 회원국의 국내법이 협약을 준수하고 있는지 여부를 평가하고 조치가 효과적인지 결정한다. 또한 제3국으로의 개인정보 이전을 위한 법적 규범이 충분한 수준의 보호를 보장하는지도 평가한다.

우리나라도 유럽평의회의 108호 협약에의 가입을 검토할 필요가 있다. 108호 협약은 개인정보 분야에서 유일하게 법적으로 구속력 있는 국제협약으로서, 국내 개인정보 보호 법제를 국제적인 규범과 조화시키고 국제적인 개인정보 협력체제에서 한국이 일정한 리더쉽을 발휘할 수 있기 때문이다.[34] 물론 108호 협약을 위해서는 국내 개인정보 보호 법제가 108호 협약의 기준을 충족하는지 검토할 필요가 있다. 프로파일링 등 자동화된 의사결정과 관련한 정보주체의 권리 보장, 설계 및 기본설정에 의한 개인정보 보호, 개인정보 영향평가 등 개인정보처리자의 책임성을 강화할 수 있는 조치들, 다른 국가에서 우리 국민의 개인정보가 안전하게 보호될 수 있도록 보장하면서 개인정보 이전이 다양한 방식으로 이루어질 수 있도록 하는 개인정보 국제이전 조항의 보완 등이 이루어져야 할 것으로 보인다.

34) 박훤일, 앞의 글, pp199-200.

제2절 주요 국가의 개인정보 보호 법제

1. 유럽연합

가. 유럽연합의 개인정보 보호법제

유럽연합은 2000년에 <유럽연합 기본권 헌장(the Charter of Fundamental Rights of the European Union)>을 선포하였다. 이는 유럽연합의 정책이 인권에 미치는 영향에 대한 인식과 함께 유럽 시민들이 유럽연합을 보다 가깝게 느끼도록 하기 위한 노력의 일환이었다. 헌장은 처음에는 정치적인 문서였지만, 2009년 12월 1일 리스본 조약이 발효된 이후 법적 구속력이 있는 유럽연합의 기본법(primary law)이 되었다. 유엔의 시민적, 정치적 권리에 관한 국제규약(ICCPR), 유럽평의회의 유럽인권조약과 달리 유럽연합 기본권 헌장은 사생활 및 가족생활에 대한 존중(7조)뿐만 아니라, 개인정보 보호의 권리(8조)를 명시하고 있다. 헌장은 1995년에 채택된 개인정보보호 디렉티브 이후에 만들어졌기 때문에, 개인정보 보호의 권리에 대한 언급(1항)과 함께, 공정한 처리, 목적 명확화, 동의 혹은 다른 적법한 근거, 정보주체의 접근 및 정정권 등 기본적인 원칙을 규정(2항)하고 있으며, 이러한 원칙 준수를 감독할 수 있는 독립적인 기관의 설립(3항)도 요구하고 있다[35].

유럽연합 기능에 관한 조약(Treaty on the Functioning of the European Union : TFEU) 제16조는 모든 사람은 개인정보 보호의 권리를 갖고 있으며(1항), 유럽의회 및 유럽연합 이사회(Council of the European Union)로 하여금 개인정보 처리에 대한 개인의 보호와 관련된 규범을 수립하도록(2항) 함으로써, GDPR 및 '경찰 및 형사사법당국을 위한 디렉티브' 등 유럽의 개인정보 보호 규범의 포괄적 개혁안 채택의 법률적 근거가 되고 있다.

최근 GDPR 시행 이전까지 유럽연합의 주요 개인정보 보호 법제는 1995년 10월 채택된 개인정보보호 디렉티브(95/46/EC)였다. 이 디렉티브를 만든 이유는 당시 일부 국가들이 이미 개인정보 보호와 관련된 국내 법률을 갖고 있었는데, 회원국 사이의 개인정보

35) EU 법제 개관에 대해서는 FRA(2018a) , pp27-35 참조.

보호와 개인정보의 자유로운 이동을 보장할 수 있는 법제의 통일 필요성이 대두되었기 때문이다. 이 디렉티브는 기존 각국의 법률과 유럽평의회 108호 협약을 기본으로 하면서, 이를 확대하였다. 특히 개인정보 보호 규범에 대한 준수를 강화하기 위해 독립적인 감독기관을 도입했는데, 이는 2001년에 108호 협약 추가 의정서 채택에 영향을 주었다. 이처럼 유럽연합과 유럽평의회의 규범들은 상호 작용을 하면서 긍정적인 영향을 미치고 있다.

그러나 유럽연합의 법제 구조상, 디렉티브는 직접적인 효력을 가지는 것이 아니라 회원국의 국내법에 반영이 되어야 한다. 이에 따라 디렉티브가 회원국 간의 법제 조화를 목표로 했음에도 불구하고, 실제로는 회원국 사이에 서로 다른 방식으로 법제화되었다. 집행이나 제재의 수준도 나라마다 편차가 있었다. 한편, 90년대 중반 이후 정보통신기술은 상당한 발전을 이루었고 개인정보 보호 규범에도 이러한 변화를 반영할 필요성이 제기되었다. 이러한 개혁 요구들이 2016년 4월 GDPR의 채택으로 이어졌다. GDPR은 2년 동안의 준비 기간을 거쳐 2018년 5월 25일 발효되었다.

한편, 범죄 수사 영역에서 개인정보 보호와 관련한 규범은 유럽평의회가 1987년에 제정한 '경찰 권고(Recommendation (87)15)'가 있었지만, 유럽연합의 개인정보보호 디렉티브는 경찰 및 형사사법 분야에 적용되지 않았기에 이 분야 개인정보 보호 규범이 모호한 상태라고 평가받았다. 이에 2016년에 '경찰 및 형사사법 당국을 위한 디렉티브(Directive 2016/680)'(일명 경찰 디렉티브)가 의결되어 2018년 5월 GDPR과 함께 발효되었다. 경찰 디렉티브는 범죄 예방・수사・탐지・기소, 형사처벌 집행 및 공공안전 보호・위험 방지 등 형사 사법 문제를 소관하는 기관이 해당 목적으로 개인정보를 수집하고 처리할 때 개인정보를 보호하는 것을 목적으로 한다[36].

유럽연합은 전자통신분야에 특화된 디렉티브로 2002년 채택된 '프라이버시 및 전자통신에 관한 디렉티브(혹은 e-Privacy 디렉티브)'를 가지고 있다(Directive 2002/58/EC)[37]. 이 디렉티브는 전자통신 네트워크에서의 개인정보 보안, 개인정보 유출시 고지, 통신의 기밀성 등을 규율한다. 2017년 1월, 유럽연합 집행위원회는 e-Privacy 디렉티브를

36) 이광석 외(2018), 앞의 글, pp147-148.

37) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications, OJ L 201 (Directive on privacy and electronic communications or e-Privacy Directive).

대체하는 새로운 e-Privacy 규정안을 채택하였다. GDPR이 유럽연합 기본권 헌장 제8조(개인정보보호)를 주로 규율한다면, e-Privacy 규정은 기본권 헌장 제7조(사생활존중권)를 유럽연합 법체계에 통합하려는 것이다. 이 규정은 이전 디렉티브의 규정을 신기술 및 시장 현실에 적용하고 포괄적이며 GDPR과 일관된 체계를 수립하고자 한다. 그런 점에서 e-Privacy 규정은 GDPR의 특별법으로서, 개인정보를 구성하는 전자통신 데이터에 그 원칙을 적용한다. 새 규정은 개인정보가 아닐 수도 있는 통신 내용 및 메타데이터를 포함하여 모든 '전자통신 데이터'의 처리를 관장하며, GDPR 집행 체제가 이 규정에도 적용된다. e-Privacy 규정은 본래 2018년 5월 25을 GDPR 시행에 맞추어 채택될 예정이었으나 현재 지연되고 있는 상황이다[38]. GDPR 2년에 대한 평가에서 유럽연합 집행위원회는 e-Privacy 규정의 빠른 채택이 필요하다는 것을 강조하고 있다[39].

그 외에 유럽연합 기구와 조직에서의 개인정보 보호를 위한 규정(Regulation No. 45/2001)을 별도로 두고 있다[40].

나. 일반개인정보보호규정(GDPR)

개인정보보호 디렉티브와 달리 GDPR은 회원국의 국내법을 통하지 않고 직접적으로 적용된다. 물론 GDPR 채택 이후 유럽연합 각국은 자국의 개인정보 보호법을 개정하였는데, 이는 한편으로는 GDPR과의 일관성을 유지하면서도 다른 한편으로는 GDPR에서 허용하고 있는 범위 내에서 각국의 재량에 따른 규범을 도입하기 위한 것이다. GDPR이 기존의 규범과 달라지는 주요 특징들은 다음과 같다.

첫째, GDPR의 제정 목적 중의 하나가 '디지털 단일시장에 적합한 통일되고 단순화된 프레임워크'를 구축하고자 한 것인데, 이를 위해 원스탑샵 메커니즘(One-Stop-Shop

38) 이광석 외(2018), 앞의 글, pp143-144.

39) European Commission(2020), COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 2020.6.24 COM(2020) 264 final, p2.

40) Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ 2001 L 8.

mechanism)을 도입하였다. 원스탑샵 메커니즘은 정보주체가 유럽연합 내 여러 국가에 흩어져 있는 경우 주 사업장이나 단일 사업장이 소속된 국가의 감독기관이 선임 감독기관의 역할을 수행하면서 다른 회원국의 감독기관과 수시로 협력함으로써 컨트롤러[41] 및 프로세서는 하나의 감독기관만을 대상으로 대응 가능한 메커니즘을 말한다[42]. 컨트롤러가 설립된 국가의 감독기관이 '주 감독기관(lead authority)'으로 기능하는데, 주 감독기관이 아닌 감독기관의 경우에도 자신의 관할 지역에서 해당 컨트롤러와 관련하여 발생한 사안을 처리할 수 있다. 해당 지역의 감독기관이 주 감독기관에 관련 사안을 통지하면 주 감독기관은 자신이 해당 지역의 감독기관과 협력하여 처리할 것인지, 아니면 해당 지역의 감독기관이 처리하게 할 것인지 결정해야 한다[43].

둘째, GDPR은 정보주체의 권리를 강화하였다. 개인정보의 정의는 기존 디렉티브와 크게 달라지지 않았지만, IP 주소와 같은 온라인 식별자(online identifier)를 개인정보 정의 규정에 명시하였고, 생체인식정보와 유전정보를 민감정보에 포함하였다. 자유롭게 주어지고, 특정되며, 정보에 기반(freely given, specific and informed)하도록 한 기존 동의의 정의에 모호하지 않아야 한다(unambigous)는 조건이 추가되었고, 제7조에서 유효한 동의의 요건, 제8조에서는 정보사회 서비스와 관련하여 아동의 동의가 유효하기 위한 조건을 상세하게 규정하였다. 이전 지침에서 규정되어 있었던 정보주체의 권리도 GDPR에서 더욱 강화되거나 세부적으로 규정되었다. 예를 들어, 개인정보보호 디렉티브에서는 삭제권과 관련하여, 부정확성, 불완전성을 근거로 정보주체가 삭제를 요구할 수 있다는 것만 규정되어 있었는데, GDPR에서는 삭제권을 행사할 수 있는 조건을 추가하는 동시에, '표현과 정보의 자유에 대한 권리의 행사'와 같이 삭제 요청을 거부할 수 있는 근거도 추가되었다. 정보주체의 열람권의 경우, 보관기간, 권리의 존재여부, 정보의 출처, 처리의 결과 등 기존 디렉티브에는 규정되지 않았던 추가적인 정보들을 열람할 수 있도록 보완되었다. 또한 새로운 정보주체의 권리로서 개인정보 이동권(right to data portability)이 추가되었는데, 이는 자신의 개인정보를 기계 판독이 가능한 형태로 제공 받거나 다른 컨트롤러에게 이전할 수 있는 권리이다.

---

41) 우리나라 개인정보 보호법의 개인정보처리자와 GDPR의 컨트롤러는 유사하기는 하지만, 개념이 조금 다르기 때문에 이 글에서 GDPR 조항을 설명할 경우에는 개인정보처리자가 아니라 컨트롤러 개념을 직접 사용하였다.

42) 한국인터넷진흥원(2020), 우리 기업을 위한 2020 EU일반개인정보보호법(GDPR) 가이드북.

43) GDPR 전문 127.

셋째, 컨트롤러의 책임성을 강화하기 위한 다양한 조치도 도입되었다. 우선 개인정보 보호와 관련하여 컨트롤러를 자문하고 감독하는 지위를 가진 독립 개인정보 책임자(Data Protection Officer, DPO)를 도입하였는데, 정보주체에 대한 대규모의 정기적이고 체계적인 모니터링을 요구하는 처리, 대규모의 민감정보 처리, 공공기관에 의해 수행되는 처리의 경우 DPO를 의무적으로 지정해야 한다. 또한 GDPR의 준수를 보장하고 입증하기 위한 조치의 하나로서 침해 위험이 큰 처리 활동에 대해서는 개인정보 영향평가를 수행하도록 하였다. 설계 및 기본설정에 의한 개인정보 보호는 효과적인 개인정보 보호를 위한 내부 정책 및 이행 조치를 취할 일반적인 의무를 컨트롤러에게 부여한다. GDPR 준수 입증을 위한 또 하나의 의무로서 개인정보 처리활동에 대한 기록을 유지하도록 하였다. 이러한 조치들은 모두 기존의 개인정보보호 디렉티브에는 없었던 새로운 책임성 강화 조치들이다. 개인정보 처리원칙에서도 기존 디렉티브에서는 단지 이러한 원칙의 준수를 보장해야 한다고 규정했으나, GDPR에서는 컨트롤러가 준수에 책임이 있고 이를 입증할 수 있어야 한다고 컨트롤러의 책임성을 강조하고 있다. 또한 디렉티브는 컨트롤러만을 언급하고 있지만, GDPR은 컨트롤러와 함께 프로세서의 책임도 규정하고 있다.

넷째, 위험성이 큰 개인정보 침해 사고가 발생한 경우, 감독기관 및 정보주체에게 통지하도록 하는 개인정보 침해통지 제도도 확대하였고, 규범 위반에 대한 제재도 강화하였다. 이에 따라 GDPR 규정의 일반적 위반의 경우 직전 회계연도의 전 세계 매출액 2% 또는 1천만 유로 중 더 큰 금액을, 심각한 위반의 경우에는 직전 회계연도의 전 세계 매출액 4% 또는 2천만 유로 중 더 큰 금액을 과징금으로 부과할 수 있도록 하였다. 기존 디렉티브와 달리 GDPR에서 정보주체는 컨트롤러뿐만 아니라 프로세서에게도 보상을 요구할 수 있다. 또한 디렉티브와 달리 GDPR은 권리 침해에 대한 사법적 구제를 정보주체의 ‘권리’로 규정하고 있다. 개인정보 감독기관의 위상과 권한도 기존 디렉티브에 비해 더욱 상세하게 규정하고 있다.

다섯째, GDPR은 사실상 전 세계에 영향을 미치는 국제규범이 되고 있다. 우선 GDPR은 유럽연합 역내에 위치한 기업이나 기관뿐만 아니라 유럽연합의 정보주체에게 재화나 용역을 제공하거나 이들의 활동을 모니터링하는 등, 유럽연합 시민의 개인정보를 수집하는 경우 유럽연합 역외의 기업에도 적용된다. 따라서 유럽연합 시민의 개인정보를 처리하는 전 세계 기업 및 기관도 GDPR 준수를 검토할 필요가 있다. 또한 GDPR은 유럽연합

시민의 개인정보가 역외의 제3국으로 이전될 경우에도 개인정보가 보호될 수 있도록, 역외 이전을 위한 다양한 제도를 마련해놓고 있다. 적정성 결정을 통해 제3국의 개인정보보호 수준이 유럽연합과 실질적으로 동등하다고 인정되는 경우, 혹은 구속력 있는 기업규칙(Binding Corporate Rules), 표준 개인정보보호 조항(Standard data protection clauses), 승인된 행동 규약(Code of Conduct) 및 인증(Certification) 등 적절한 보호조치를 제공하는 경우, 기타 정보주체의 명시적인 동의 등 예외적인 경우가 이에 해당한다. 유럽연합은 적정성 결정을 위한 협의를 통해 제3국이 유럽연합과 유사한 방식으로 법제를 개선하도록 유도하고 있다.

다. GDPR 시행 2년의 평가

GDPR 제97조는 집행위원회로 하여금 발표 만 2년이 되는 2020년 5월 25일까지 이 규정에 대한 평가 및 검토 보고서를 제출하도록 하고 있다. 평가와 검토 보고서는 이후 4년마다 제출해야 한다. 특히 적정성 결정에 따른 개인정보의 제3국으로의 이전에 대한 5장 및 협력과 일관성 메커니즘에 대한 6장을 검토하도록 하고 있다(제97조 2항). 평가과정에서 각국의 감독기관 등 여러 이해당사자의 의견을 요청할 수 있다. 또한, 필요할 경우 GDPR 규정에 대한 개정 제안을 제출해야 한다(제97조 5항). 이에 따라 집행위원회는 GDPR에 대한 첫번째 평가를 수행하고 그 보고서를 공개하였다[44]. 이 과정에서 유럽개인정보보호이사회(EDPB)도 평가 의견[45]을 제출하였고, 정보인권 옹호 시민단체인 엑세스나우(Access Now)도 시민사회 관점에서의 GDPR에 대한 평가 보고서[46]를 공개하였다. GDPR의 일부 규정을 국내 법제에 도입할 것인지 여부를 검토할 때, 실제적인 효과나 문제점을 판단하기 위해 GDPR 2년의 평가 보고서를 검토하는 것이 도움이 될 것으로 보인다.

---

44) European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 2020.6.24. COM(2020) 264 final.

45) EDPB(2020), Contribution of the EDPB to the evaluation of the GDPR under Article 97.

46) Access Now(2020), TWO YEARS UNDER THE EU GDPR.

1) 총평

집행위원회는 우선 GDPR이 디지털 전환과 그린 뉴딜을 위한 여러 사업들의 기반이라는 점을 강조하고 있다. 신기술 환경에서 개인정보 보호 규범에 대한 정립과 신뢰가 없다면 디지털 경제의 발전도 불가능하기 때문이다[47]. GDPR 시행과 관련해서는 2년의 기간은 아직 어떤 확고한 결론을 내리기에는 이른 시점이지만, 개선해야 할 점이 있음에도 불구하고 GDPR 제정 목적을 달성했다는 것이 대체적인 견해라고 평가했다. EDPB 역시 GDPR 이행에 긍정적인 평가를 내리며 아직 개정을 논의하기에는 이른 시점이라는 의견이다.

2) GDPR의 집행

가) 집행 권한의 활용

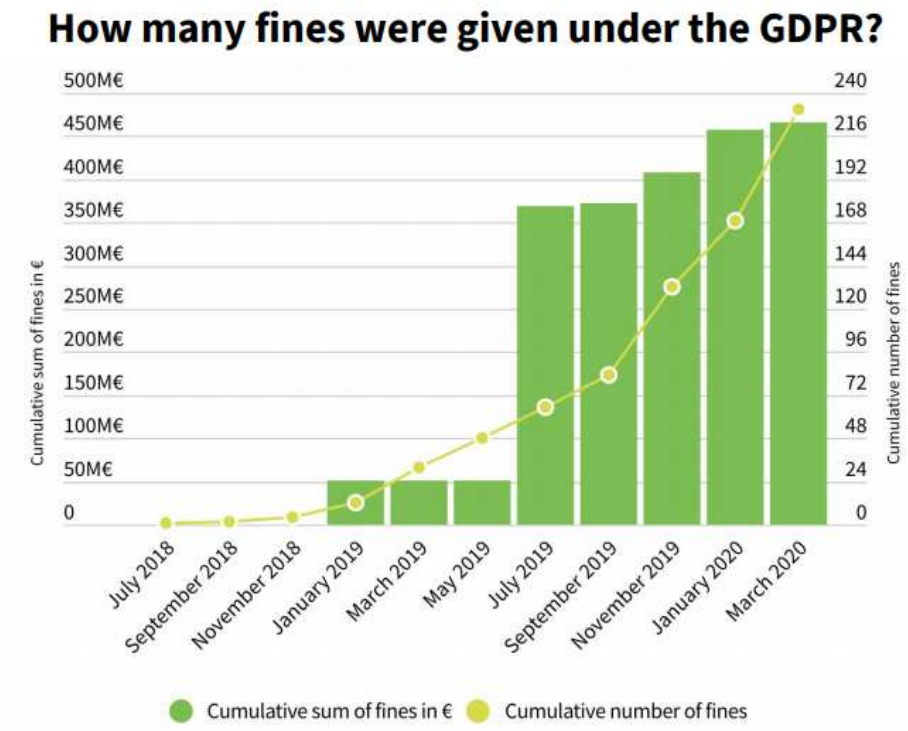
집행위원회는 감독기관들이 경고, 질책(reprimand), 과징금(fines), 임시적/최종적 처리 제한 등 강화된 자신의 권한을 균형 있게 사용해왔다고 평가했다. 침해의 정도에 따라 과징금의 경우 수천 유로에서 수백만 유로가 부과되기도 했다.

EDPB에 따르면, 2019년 11월까지 총 275,557건의 진정(complaint)이 제기되었다. 22개의 감독기관들이 785건의 과징금을 부과하였고 8개 감독기관은 아직 과징금을 부과한 적은 없지만 과징금을 부과할 수 있는 분쟁을 처리 중이라고 한다. 감독기관들의 실제 경험에 근거한 의견에 따르면 다음과 같은 요소들이 과징금 액수에 영향을 미친다고 한다. 감독기관과의 협력의 정도, 침해가 체계적·반복적인 성격을 가지고 있는지 여부, 의도성 여부, 컨트롤러가 문제를 시정하고 향후 침해 방지를 위해 취한 조치, 침해의 성격과 지속기간, 과거에 관련된 침해가 있었는지, 컨트롤러의 성격(즉, 산업분야의 전문성, 대중적 인지도 등), 개인정보의 종류, 영향을 받은 정보주체의 수 등이다.

반면, 엑세스 나우는 GDPR 발효 이후 2019년에 집행 활동이 급증하기는 했지만, 시장과 이용자는 그 영향력을 아직 느끼지 못하고 있다고 평가했다. 2020년 3월까지 부과된

47) 유럽연합은 디지털 시대에 적합한 유럽(Europe fit for the digital age)과 유럽 그린딜(European Green Deal) 사업을 위한 기본 틀로서 GDPR을 인식하고 있는데, 이는 최근 디지털 뉴딜과 그린 뉴딜로 이루어진 한국형 뉴딜 사업을 추진하고 있는 한국에 시사하는 바가 많다.

<그림2-1> 시기별 과징금 건수와 액수



* 출처: 엑세스 나우

과징금 건수는 231건으로 제기된 진정에 비하면 매우 낮은 수준이다. 그리고 감독기관은 넘쳐나는 진정을 감당하지 못하고 여전히 많은 진정이 적체되어 있는 상황이다. 더구나 아마존, 페이스북, 왓츠앱, 트위터, 페이팔, 인스타그램, MS, 구글 등의 분쟁을 다루는 아일랜드와 룩셈부르크의 감독기구는 아직 이들 기업에 과징금을 부과한 바가 없다. 2018년과 2019년 아일랜드의 감독기관은 총 11,328건의 진정을 받았다고 한다.

나) 협력 및 일관성 메커니즘

집행위원회는 평가하기에는 이르다면서도 감독기관들이 원스탑샵 메커니즘(60조) 및 상호 지원(61조)을 통해 협력을 발전시켜왔다고 보았다. 주로 거대 기술기업과 관련된, 다국적인 차원에서 중요한 결정들도 대기 중이다. 그러나 감독기관 간의 공통의 개인정보 보호 문화 형성은 계속 진행 중인 과정이며, 감독기관들이 공동 조사 등을 포함한 공

동 작업(Joint operation) 등 GDPR에서 규정한 수단들을 최대한 활용하지는 못하고 있다고 평가했다. EDPB 보고서에 따르면, 62조 공동작업은 아직 한 번도 활용된 바가 없다.

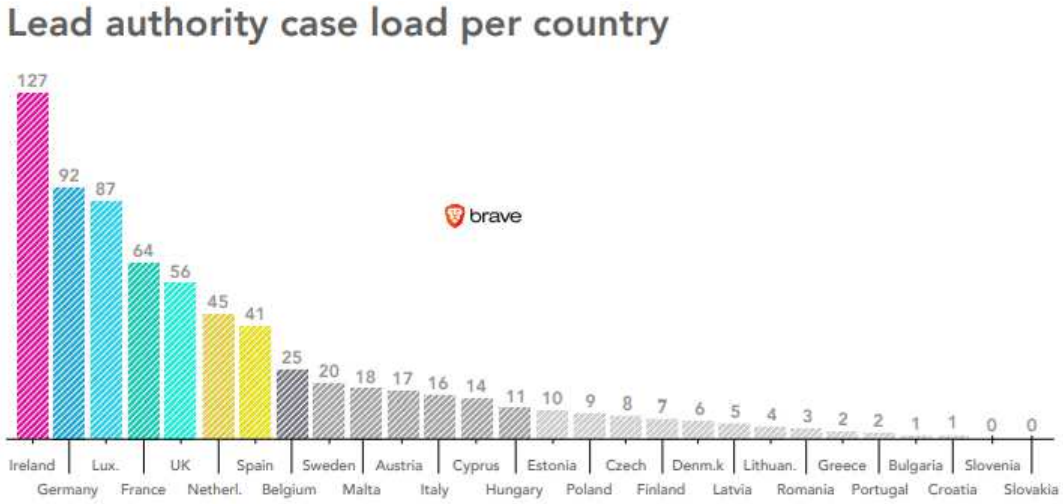
또한 집행위원회는 국경간 분쟁의 효과적인 처리를 위한 개선이 필요하다고 지적했는데, EDPB 역시 같은 평가를 내리고 있다. 예를 들어, 진정 처리 절차를 포함하여 국내 절차나 관행이 서로 다른 문제, 진정을 허용하는 기준, 절차가 진행되는 기간, 마감 기간의 차이, 당사자 의견을 듣는 절차, 진정인의 참여권 허용 여부 등이다. 또한 EDPB는 협력 메커니즘과 관련한 개념에 대해 감독기관들이 서로 다른 해석을 하고 있는 것도 문제로 지적했다. 예를 들어, '관련 정보', '지체 없이', '결정 초안', '원만한 해결' 등에 대한 구체적인 해석이 다르다는 것이다. EDPB는 전문가 그룹을 구성하여 핵심 개념에 대한 공통 해석을 위한 작업을 진행 중이다.

한편, EDPB는 감독기관 사이의 원활한 상호작용을 위해 내부시장정보(Internal Market Information, IMI) 시스템을 운영 중이며, 제60조에 따른 공식적인 원스탑샵 절차뿐만 아니라 그 이전에 감독기관의 비공식 협의를 비롯한 여러 단계의 절차를 제공하고 있다. 국경간 분쟁은 모두 중앙의 데이터베이스에 등록이 된다고 한다.

GDPR의 일관된 적용(일관성 메커니즘)을 위해서는 EDPB의 역할이 중요하다. 2019년 12월까지 EDPB는 제64(1)조에 따른 의견서를 36개, 제64(2)조에 따른 의견서(한 개 이상의 회원국에서 적용되는 문제에 대한 EDPB의 의견서)를 6개 채택했는데, 64(1)조에 따른 의견서 중 31개가 35(4)조 개인정보 영향평가를 받아야 하는 개인정보 처리에 대한 것이다. EDPB는 감독기관들이 EDPB의 의견을 수용하는데 아무런 문제가 없었으며 GDPR의 일관된 해석에 도움이 되어 왔다고 평가하였다. 그러나 EDPB의 의견서가 유럽경제지역에 적용되는 특정한 주제를 다룰 수 있다면 더욱 효과적일 것이며, 개인정보 영향평가 목록에 대해 31개의 의견을 내는 것을 피할 수 있을 것이라고 제안했다.

그러나 시민단체인 엑세스 나우는 긍정적인 평가를 유보하며 원스탑샵 시스템이 국경간 분쟁을 효과적으로 해결할 수 있을지 의문을 제기했다. 컨트롤러에게는 원스탑샵(one-stop-shop)이지만 정보주체에게는 '쓰리스탑샵(three-stop-shop)'일 수 있다는 GDPR 채택 이전의 비판이 현실이 될 수도 있다는 것이다. 이를테면, 일부 감독기관은 주 감독기관이 투명하지도 않고 진정을 빨리 처리하지 않는다고 비판한다. 감독기관의 부족한 예산과 자원도 협력의 주요 장애물이다. 기관간 협력을 요하는 사건을 원활히 처

<그림2-2> 국가별 주 감독기관이 되는 분쟁 사례



* 출처: brave 보고서

리하기에는 예산과 인력이 부족하다는 것이다.

또한 엑세스 나우는 원스탑샵 메커니즘에 따라, 많은 거대 기술기업이 등록되어 있는 아일랜드의 감독기구 DPC가 주 감독기관으로서 GDPR 적용의 핵심적인 역할을 맡고 있는데, 이에 따라 행정적인 문제도 발생하지만 잠재적으로 정치적인 이슈가 될 수 있다고 지적하고 있다. 아일랜드는 거대 기술기업의 조세피난처가 되어 왔고 이에 따라 이들 기업들이 아일랜드의 정책에 많은 영향을 미치고 있는데, 이제 개인정보의 집행이 로비의 타겟이 되고 있다는 것이다. 이에 따라 DPC가 기업과 정부의 압력에도 불구하고 독립적으로 자신의 권한을 충분히 행사할 수 있을지가 관건이다. 현재 DPC는 몇 개의 조사를 개시하기는 했지만, 아직 주요 결정은 나오지 않은 상황이다.

엑세스 나우는 감독기관간 협력과 일관성을 위해 집행위원회와 EDPB의 역할이 핵심적이라고 지적하면서, 또한 감독기관들이 제66조 '긴급 절차'의 활용을 시작할 것을 촉구하였다. 긴급 절차는 협력 및 일관성 메커니즘 하에서 주 감독기관이 제 역할을 하지 못할 때 진정이 제기된 지역의 감독기관이 자신의 관할권 내에서 임시적인 조치를 취할 수 있도록 한다. 원스탑샵 메커니즘이 제대로 작동하지 않을 때, 감독기관이 정보주체의 권리 보호를 위해 적극적인 조취를 취해야 한다는 요구이다.

다) 감독기관의 자원 부족

감독기관이 자신의 역할을 제대로 수행하기 위해서는 인적, 재정적 자원이 제대로 지원되는 것이 핵심적이다. 그러나 감독기관 전반적으로 인적, 재정적으로 부족한 상태이며, 회원국 간에도 불균등하다는 것이 집행위원회, EDPB, 엑세스 나우 등의 공통된 평가이다.

집행위원회도 2016년에서 2019년까지 감독기관 대부분의 인력 및 재정이 증가해 왔음에도 불구하고 여전히 만족스럽지 않고 회원국 간 불균등하다고 인정하고 있다. EDPB 역시 GDPR의 적용과 원스탑샵의 성공은 감독기관의 자원에 의존적인데, 설문조사 결과 대부분의 감독기관들이 자원이 부족하다고 답변했다고 보고했다. 또한 감독기관의 대부분은 GDPR이 부과한 업무뿐만 아니라 경찰 디렉티브 및 e-Privacy 프레임워크와 관련된 책임을 맡고 있다고 한다.

엑세스 나우는 감독기관은 GDPR이 성공할 수 있느냐의 핵심적인 요인이지만, 자원 부족에 시달리고 있다고 비판했다. 2018년에 비하여 2019년에 감독기관의 피고용인 수가 거의 증가하지 않았으며 2020년에도 거의 같은 수준일 것이라고 보았다.

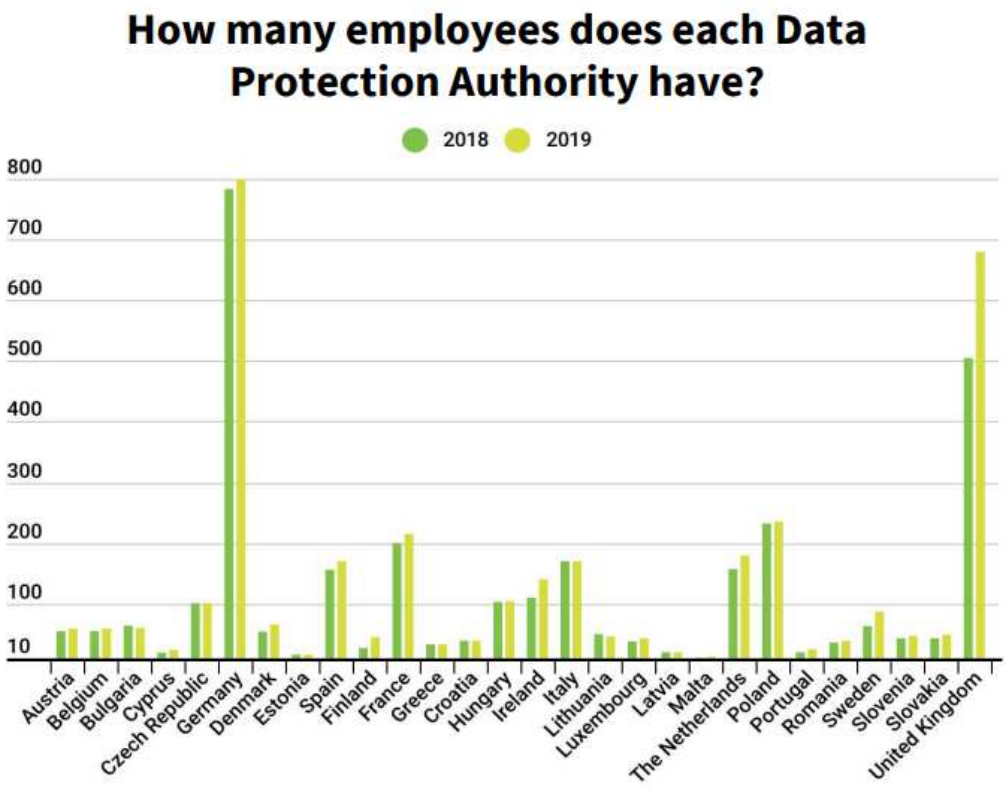
감독기관 사이에 예산의 차이도 많이 나고 있다. 독일이 가장 많지만, 이는 독일의 주와 연방의 17개 감독기관을 합한 것이다. 개별 감독기관으로는 영국의 ICO가 피고용인과 재정이 가장 풍족하다. 그래서 감독기관간 협력에 영국 ICO가 많은 지원을 하고 있는데, 영국이 유럽연합을 탈퇴하게 되면 이런 지원이 축소될 것이라고 지적했다. 엑세스 나우는 감독기관의 자원이 부족할 경우, 법 집행이 안 되고 법이 무시되는 상황이 벌어질 수

<그림2-3> 자원이 충분한 지 여부에 대한 감독기관들의 답변

HR, Financial, Technical resources	SAs
The resources are not enough	AT, BE, BG, DE[4], EE, ES, FI, FR, GR, IE, IS, IT, LT, LV, MT, NL, PT, PL, RO, SK, SI
The resources are enough	CY, CZ, DK, HR, HU, LU, NO, SE, UK

* 출처: EDPB 보고서

<그림2-4> 감독기관의 피고용인 수



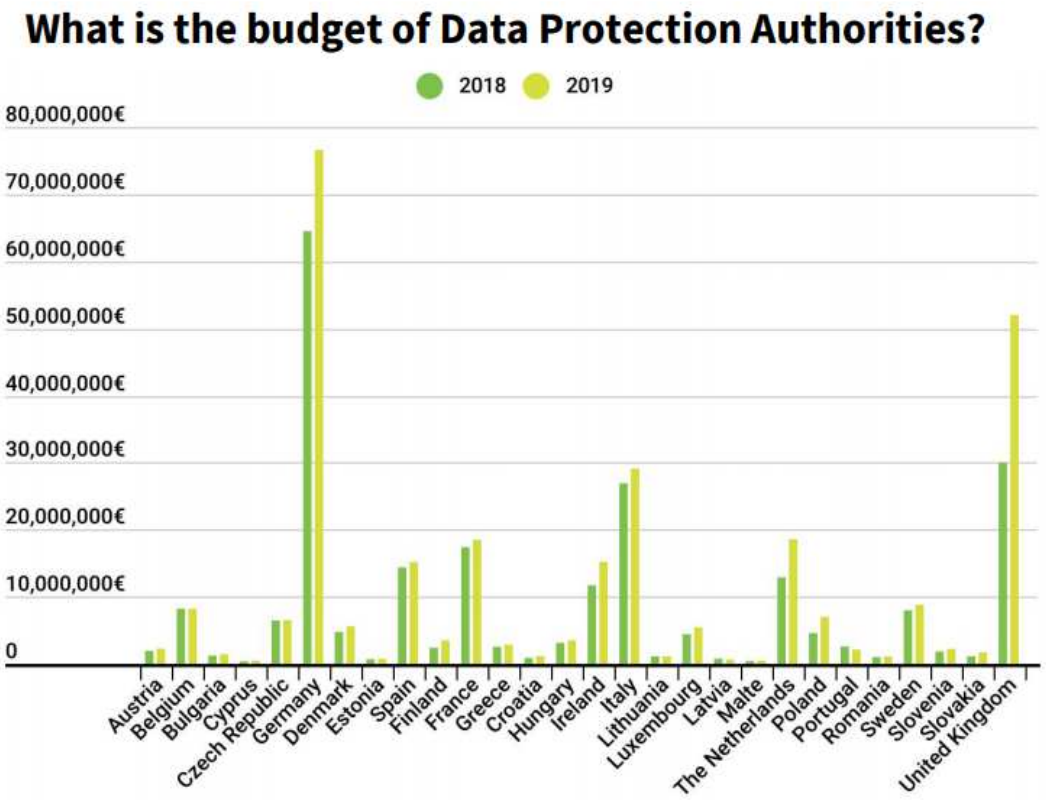
* 출처: 엑세스 나우 보고서

수 있다고 경고한다. 특히 자원이 풍부한 거대 기술기업과 소송이 벌어졌을 때 감독기관의 자원이 부족하면 장기간의 소송을 벌이는 것보다 기업에 유리한 합의를 할 가능성을 우려하고 있다.

브레이브(Brave)라는 오픈소스 브라우저를 개발하고 있는 업체는 대부분의 감독기관들이 기술적인 집행 역량이 부족한 점을 지적하며 GDPR이 실패하고 있다고 진단했다[48]. 특히 거대 기술기업과 상대하기 위해서는 감독기관들이 충분한 자원과 함께 전문적인 기술 역량을 보유하고 있어야 한다. 그러나 브레이브의 보고서에 따르면, 6개 감독기관만이 10명 이상의 기술 전문가를 보유하고 있으며, 7개 감독기관이 보유하고 있는 기술 전

48) Brave(2020), Europe's governments are failing the GDPR - Brave's 2020 report on the enforcement capacity of data protection authorities.

<그림2-5> 감독기관의 예산



* 출처: 엑세스 나우 보고서

문가는 2명 이하이다. 영국의 ICO는 가장 많은 인력을 보유하고 있지만 단지 3%만이 기술 전문가이다. ICO의 예산은 프랑스 감독기관인 CNIL의 3배이지만 CNIL이 더 많은 기술 전문가를 보유하고 있다. 유럽연합 기술 전문가의 1/3인 29%가 독일의 주 및 연방 감독기관 소속이다.

3) 개인정보 규범의 조화

현재 슬로베니아를 제외한 모든 회원국이 새로운 개인정보 보호법을 채택했다고 한다. GDPR 제정의 주요 목적 중의 하나가 유럽연합 역내에서 통일적인 단일 규범을 적용하는 것이었지만, GDPR 역시 일부 조항에서는 각 회원국의 자율성을 부여하고 있다. 그 결과 일정하게 분절(fragmentation)이 여전히 남아있다. 대표적인 사례가 정보사회 서비

스에 동의할 수 있는 아동의 연령 문제이다.

또 하나의 문제는 개인정보 보호와 표현의 자유 사이의 조화 문제이다. 일부 국가는 표현의 자유에 우위를 두는 반면, 다른 나라는 개인정보 보호에 우위를 두고 있다. 집행위원회는 각국의 법률들을 계속 평가할 예정이라고 한다. 집행위원회는 언론인에게 정보원을 요구하는 등 개인정보 보호를 명분으로 표현의 자유 행사에 영향을 주어서는 안 되며, 두 권리의 균형은 유럽사법재판소와 유럽인권재판소의 판례에 구속된다고 지적한다.

이와 관련하여 엑세스 나우도 많은 공공기관이 언론의 자유나 시민사회 활동을 제약하기 위해 GDPR을 남용하고 있다고 비판하고 있다. 여러 사례를 제시하고 있는데, 예를 들어 헝가리에서는 기업 소유자의 개인정보 침해를 명분으로 헝가리 부자들 목록을 다룬 포브스 잡지를 수거하라는 명령이 떨어졌다고 한다. 폴란드에서는 국립법원등록소의 데이터를 포함하여 공공 등록소의 데이터 검색 엔진을 통해 공공정보에 대한 접근을 제공했다는 이유로 한 비영리단체에 GDPR 위반 진정이 제기되었다고 한다.

한편, 건강 및 연구 목적으로 민감정보의 처리 금지 예외를 설정할 때, 세부적인 사양이나 안전조치의 수준에 있어서 회원국 사이에 서로 다른 접근을 취하고 있다. 집행위원회는 이에 대해 상황을 파악하고 있으며 일관된 접근을 위한 행동 규약을 수립할 예정이라고 한다. 또한 과학적 연구를 위한 개인정보 처리와 관련하여 EDPB의 가이드라인이 나오면 보다 조화로운 접근이 가능할 것이라고 한다.

4) 정보주체의 자기정보 통제권의 강화

집행위원회는 개인들이 자신의 권리를 점차 인지해가고 있으며, GDPR은 절차적인 권리도 강화했는데 대표소송에 관한 디렉티브(Directive on representative actions)[49]가 채택되면 각 회원국에서 집단 소송을 활성화하고 국경간 소송 비용을 낮출 수 있을 것으로 전망했다.

또한, 개인정보 이동권은 이용자가 서비스를 다른 서비스 제공자로 교체하고, 서로 다른 서비스를 결합하고, 다른 혁신적인 서비스를 사용하고, 가장 개인정보 친화적인 서비

49) Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC COM/2018/0184 final - 2018/089 (COD).

스를 사용하여 개인이 데이터 경제의 중심이 될 수 있도록 할 잠재력이 있지만, 아직 많이 사용되고 있지 않다고 평가하면서, 이 잠재력을 발전시키는 것이 집행위원회의 우선순위가 될 것이라고 한다. 이를 위해 적절한 도구, 표준화된 포맷, 인터페이스의 설계 등이 필요하다고 지적하며, 개인정보 이동권은 개인이 건강 분야 연구와 같은 공공의 이익을 위해 자신의 개인정보 활용 허락을 쉽게 할 수도 있다고 전망했다.

5) 조직(특히 중소기업)의 기회와 위협

집행위원회는 일부 이해관계자 보고서에서 GDPR의 적용이 특히 중소기업에게 위협이 된다고 지적했지만, 위험기반 접근에 따르면 기업 규모에 따라 예외를 적용하는 것은 부적절하다고 보았다. 다만, 일부 감독기관들이 개인정보 침해 위험이 적은 중소기업들의 GDPR 이용을 돕기 위한 실용적인 도구를 제공하고 있으며 이러한 노력이 확대되어야 한다고 제안했다.

6) 새로운 기술에의 GDPR 적용

집행위원회는 GDPR이 기술중립적이기는 하지만, 기존의 원칙을 인공지능, 블록체인, 사물인터넷, 얼굴인식 등 특정 기술에 어떻게 적용할지 명확히 할 필요가 있고 계속적인 모니터링이 필요하다고 지적했다. 예를 들어, 집행위원회의 인공지능 백서는 원격 생체인식 식별 목적의 인공지능 활용을 정당화할 조건에 대한 공개적인 토론을 제기하고 있다. 또한, 온라인 광고와 마이크로 타게팅을 포함한, 거대 디지털 플랫폼 기업에 대한 강력하고 효과적인 GDPR 집행은 개인을 보호하는 핵심적인 요소임을 강조했다.

7) 현대적인 국제 개인정보 이전 도구모음(toolbox)의 개발

GDPR은 개인정보의 국제적인 이전을 위한 여러 가지 도구들을 제공하고 있다. 우선 적정성 결정과 관련해서 유럽연합은 2019년 2월 일본과 적정성 결정을 체결하였으며, 한국과는 진전된 단계(advanced stae)이며 아시아 및 남미 국가들과 모색을 위한 대화(exploratory talk)를 진행 중이라고 평가했다. 또한 한국과의 적정성 결정 절차를 가급적 빨리 마무리하겠다고 밝혔다. EU를 탈퇴하는 영국과도 적정성 평가를 진행 중이며, 개인

정보보호 디렉티브 하에서 적정성 결정을 받은 국가와도 추가적인 안전조치를 협의했다고 한다. 그러나 2020년 7월 16일, 미국과의 프라이버시 쉴드를 무효화한 유럽사법재판소 결정은 일부 적정성 기준에 대한 명확성을 제공할 수 있기 때문에, 집행위원회는 재판소의 결정을 고려하여 기존의 적정성 결정을 평가할 것이라고 밝혔다.

적정성 결정과 관련하여 EDPB는 GDPR 하에서 유일한 적정성 결정을 체결한 일본의 경우, EU에서 이전되는 개인정보에 적용되는 추가적인 규칙이 결합되었는데, 이러한 추가 규칙이 구속력을 가지고 효과적으로 적용되는지가 이 적정성 결정의 핵심이므로 이에 대한 모니터링이 필요하다고 지적하였다. 또한 EDPB는 집행위원회가 일본의 사례와 같은 추가적인 규칙에 의존하는 적정성 구조가 지속가능하고 신뢰할 수 있는 시스템인지 보장할 필요가 있다고 촉구하였다. 이러한 추가 규칙이 필요한 이유는 제3국의 개인정보보호 법제가 GDPR과 일정한 간극이 있다는 것을 의미하는 것인데, 한국의 경우에도 GDPR의 적정성 기준에 비추어 미흡한 부분이 존재[50]하기 때문에 이러한 평가를 신중하게 검토할 필요가 있다.

한편, 집행위원회는 GDPR의 요구 조건을 반영하여 표준계약조항(SCC)의 현대화 작업도 하고 있는데, EDPB도 현재의 SCC는 개인정보보호 디렉티브 하에서 채택이 되었기 때문에 법적 및 운영상의 문제가 발생할 수 있으므로 업데이트되어야 한다고 지적했다.

8) 개인정보 분야의 수렴(convergence) 및 국제 협력의 증진

집행위원회는 GDPR을 모델로 하여 전 세계의 개인정보 보호 법제가 수렴되는 현상을 바람직한 것으로 평가하며, 그러한 방향에서 글로벌한 대화를 강화하겠다고 밝혔다. 또한 유럽연합의 데이터 전략은 신뢰할 수 있는 파트너와 데이터의 공유를 증진하는 동시에, 공공기관에 의한 개인정보의 무차별 접근과 같은 남용과 싸우는 것이라고 강조하였다. 또한 디지털 보호주의에 대한 반대를 표시하며 이를 위해 양자, 다자간 무역협정에서 데이터의 흐름과 개인정보 보호에 관한 특정한 조항을 포함시켰다고 밝혔다.

그러나 이에 대한 EDPB의 입장은 달라 보인다. EDPB는 국제 무역 협상에서 집행위원회는 개인정보 보호를 제외하는 관행을 유지해야 한다고 밝혔다. 또한 G20과 G7에서처럼 “신뢰할 수 있는”이 덧붙여지더라도, “데이터의 자유로운 흐름” 개념의 사용에

50) 이와 관련해서는 이은우 외(2018), 앞의 글, 제2장 제3절 및 <보론> 참조.

신중할 필요가 있다고 강조했다. 데이터의 자유로운 흐름에 대한 논의 이전에 GDPR이나 적정성 결정에 따른 추가적인 이전에 의해서 침해되지 않을 수 있는 수준으로 강력한 개인정보 보호를 제공할 필요가 있다는 것이다.

한편, 집행위원회는 유럽시장에서 활발한 기업들이 법집행 목적의 데이터 공유 요청을 받을 때, 법의 상충이나 기본권 침해 없이 그렇게 할 수 있어야 하며, 이를 위해 집행위원회는 법의 상충을 피하고 국제 협력을 위해 해외 파트너와 적절한 법적 프레임워크 개발을 위해 노력하고 있다고 밝혔다.

라. 유럽사법재판소의 개인정보 관련 주요 결정

유럽사법재판소는 회원국이 유럽연합의 개인정보 보호법 하의 의무를 수행했는지 여부에 대해 결정하고, 유럽연합 법제가 회원국에 효과적이고 일관성 있게 적용될 수 있도록 해석할 권한을 가지고 있다[51]. 그래서 유럽사법재판소의 판결은 유럽연합 법제 해석의 기준이 되어 왔으며, 때로는 재판소의 판결이 추후에 입법으로 이어지기도 했다. 개인정보와 관련된, 최근 유럽사법재판소의 주요 판결은 다음과 같다.

1) 제3국으로의 개인정보 이전과 슈렘스 판결의 의미

가) 슈렘스 I 판결과 세이프하버 협정 무효화

오스트리아 국적의 페이스북 이용자인 막스 슈렘스(Max Schrems)[52]는 2013년 6월 25일, 페이스북 유럽 지사가 소재한 아일랜드의 개인정보 감독기관인 DPC(Irish Data Protection Commissioner)에 페이스북 아일랜드가 개인정보를 미국으로 이전하지 못하도록 법적 권한을 행사해 줄 것을 요청하는 진정(complaint)을 제기하였다. 2013년 6월 에드워드 스노든이 폭로한 미국 국가안보국(NSA)의 인터넷 대량 감청 스캔들을 고려할 때 미국의 법과 관행이 적절한 개인정보 보호 수준을 제공하지 못하고 있다는 것이다. 그러

51) FRA(2018a) , p35.

52) 슈렘스는 'europe-v-facebook.org 근본적인 개인정보 보호의 실현을 위한 협회'라는 이름의 오스트리아 비영리 단체의 의장으로 활동하면서, 오래동안 페이스북의 개인정보 침해와 폐쇄적인 정책 등에 대해 비판해왔다. 이 프로젝트는 2017년에 중단되었고, 이후 슈렘스는 NOYB(My Privacy is None of Your Business)라는 디지털 권리 옹호 단체를 만들어 활동하고 있다.

나 DPC는 슈렘스의 진정을 조사할 필요가 없다고 보고 기각하였다. 슈렘스의 개인정보가 NSA에 의해 접근되었다는 증거가 없고, 유럽연합 시민의 개인정보의 미국으로의 안전한 이전 문제를 다룬 세이프하버 협정(EC 결정 2000/520)[53]에 따라 유럽연합 집행위원회가 미국의 보호 수준이 적정하다고 보장하였기 때문에 더이상 조사할 의무가 없다는 것이다. 2013년 10월 24일, 슈렘스는 DPC의 결정에 대해 아일랜드 고등법원에 행정소송을 제기하였고, 2014년 7월 17일 아일랜드 고등법원은 중간 판결을 내리며 유럽사법재판소에 주요 쟁점에 대한 사전 판결(preliminary ruling)을 요청했다[54].

2015년 10월 6일, 유럽사법재판소는 이 사건에 대한 판결을 내렸다[55]. 판결 내용은 크게 두 가지이다. 첫째 개인정보 감독기관의 권한 문제, 둘째 세이프하버 협정의 유효성 문제이다.

유럽사법재판소는 개인정보 감독기관의 독립성 보장은 법의 준수 여부 모니터링의 효과성과 신뢰성을 보장하기 위한 것이며 독립적인 개인정보 감독기관의 설립은 개인정보 보호의 핵심적 요소라고 보았다. 그리고 개인정보 감독기관은 제3국에서의 개인정보 처리와 관련된 권한은 없지만, 제3국으로의 이전은 그 자체로 유럽연합 회원국 내에서 수행되는 개인정보의 처리에 해당하므로 감독기관의 권한 범위 내에 있다. 집행위원회의 적정성 결정은 각 회원국에 적용되고 집행위원회의 결정이 무효라는 법원의 판결이 없는 한 각국은 이에 따라야 한다. 그러나 이것이 정보주체가 개인정보 감독기관에 자신의 권리 침해에 대한 진정을 하는 것을 막는 것은 아니고 마찬가지로 각 국가의 개인정보 감독기관의 권한을 줄이는 것도 아니다. 따라서 유럽사법재판소는 집행위원회가 지침 25(6)조에 따라 적정성 결정을 했다고 하더라도, 국가 개인정보 감독기관은 진정을 접수받았을 때 완전히 독립적으로 개인정보 이전이 요구조건을 만족시키는지 여부에 대해 조사할

53) 세이프 하버(Safe Harbor) 협정은 2000년 10월 16일 미국와 유럽연합이 체결한 협정으로, 이에 따르면 유럽연합에서 미국으로 개인정보의 이전을 원하는 기업들이 미국 상무부가 제정한 '세이프하버 프라이버시 원칙'과 원칙의 이행방안을 규정한 FAQ를 준수할 경우, 적정한 보호수준을 제공한다고 간주한다. 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441).

54) 슈렘스 Ⅰ판결과 관련해서는 이은우 외(2018), 앞의 글, pp45-51 참조.

55) Court of Justice of the European Union(2015), Case C-362/14, Schrems v Data Protection Commissioner.

수 있어야 한다고 판결하였다.

둘째, 세이프하버 협정의 유효성에 대한 유럽사법재판소의 판결은 적정성 결정의 의미, 적정성 결정과 관련한 집행위원회 및 개인정보 감독기관의 역할에 대한 보다 명확한 해석을 제공하고 있다. 유럽사법재판소는 각국이 개인정보를 보호하는 방법은 다를 수 있지만, 개인정보보호 디렉티브 제25조에서 규정하고 있는 '적절한 보호 수준(adequate level of protection)'은 유럽연합 헌장에 비추어 해석되는 개인정보보호 디렉티브가 보장하는 것과 실질적으로 동등한 수준으로 해당 제3국의 보호 수준을 요구하는 것으로 이해해야 한다고 보았다. 또한 디렉티브는 개인정보 이전을 둘러싼 모든 상황을 고려하도록 하고 있는 바, 이는 제3국에서 적용되는 법제뿐만 아니라 그 법제의 준수를 보장하기 위한 실제 관행을 함께 살펴보아야 한다.

그런데 세이프하버 협정(EC 결정 2000/520) 1조와 관련하여, 세이프하버 원칙은 스스로 인증한 미국의 기업에게 적용될 뿐 미국의 공공기관에는 그 준수가 요구되지 않으며, 적정한 보호 수준의 보장을 위한 미국의 조치에 관하여 충분한 규정을 포함하고 있지 않다. 또한 '국가안보, 공익, 법집행 요구 조건에 필요한 한도에서' 세이프하버 원칙의 적용이 제한될 수 있는데, 국가안보 등의 목적을 위한 개인정보 침해를 제한하기 위한 어떠한 규칙도 포함하고 있지 않으며 효과적인 법적 보호도 존재하지 않는다. 유럽사법재판소는 기본권에 대한 제한과 예외는 엄격하게 필요한 한도 내에서 적용되어야 하며, 특히 전자커뮤니케이션의 내용에 공공기관이 일반적으로 접근하도록 허용하는 법률은 기본권의 본질을 훼손한다고 보았다. 또한 개인이 자신의 정보에 접근할 가능성을 제공하지 않는 법률은 헌장 제47조에 따라 효과적인 법적 보호를 받을 기본권의 본질을 존중하지 않는 것이라고 보았다. 세이프하버 협정을 수립한 EC 결정 2000/520은 미국이 자국법이나 국제조약을 통해 사실상 동등한 보호 수준을 보장할 것을 언급하지 않았으며, 따라서 세이프하버 원칙의 내용을 살펴볼 것도 없이 EC 결정 2000/520의 제1조가 개인정보보호 디렉티브 25(6)조에서 명시한 요구조건을 준수하지 못했으므로 무효라고 판결했다.

더불어 EC 결정 2000/520의 3(1)조는 국가 감독기관의 권한을 규정하고 있는데, 국가 감독기관이 매우 제한적인 조건에서만 개입할 수 있도록 하고 있다. 이는 국가 감독기관의 권한을 부인하는 것으로 3(1)조의 채택은 집행위원회의 권한을 넘어서는 것이다. 따라

서 3조는 무효이다. 세이프하버에 대한 EC 결정 2000/520의 1조 및 3조는 2조 및 4조와 불가분의 관계이며, 따라서 1조 및 3조의 무효는 이 결정 전체의 유효성에 영향을 미치게 된다. 따라서 EC 결정 2000/520, 즉 세이프하버 협정은 무효라고 판결하였다.

유럽사법재판소는 제3국의 개인정보 보호 수준이 실질적으로 유럽연합의 보호 수준과 동등해야 한다고 보았으며, 정보수사기관 등이 개인정보에 접근할 때에도 필요성과 비례성의 원칙을 준수하고 정보주체에게 적절한 구제 수단을 제공해야 함을 중요하게 판단하고 있다는 점, 그리고 집행위원회에 의해 적정성 결정이 체결되더라도 향후에 개별 국가의 감독기관에 의해 다른 판단이 내려질 수도 있다는 점은 현재 유럽연합과 적정성 결정을 추진하고 있는 한국의 입장에서도 심각하게 고려해야 할 내용이다.

나) 슈렘스Ⅱ 판결과 프라이버시 쉴드 무효화

유럽사법재판소 판결 이후, 유럽연합 집행위원회와 미국 정부는 세이프하버 협정을 대체할 새로운 체제를 협의하였고, 2016년 7월 12일 프라이버시 쉴드 협정을 체결하였다. 미국의 기업이 프라이버시 쉴드를 이용할 경우, 우선 미국 상무부에 등록해야 하며, 미 상무부는 프라이버시 쉴드의 관리와 운영에 책임을 지며 기업들이 이를 준수하도록 보장한다. 기업에게는 '프라이버시 원칙' 의무가 적용되는데, 기업들은 이에 따라 자신의 프라이버시 정책을 수립해야 한다. 1년 단위로 회원자격을 갱신해야 하며, 그렇지 않으면 더이상 유럽연합 시민의 개인정보를 수집·이용할 수 없다[56].

프라이버시 쉴드는 미국의 공공기관이 개인정보에 접근할 때 발생하는 문제에 대한 해결책도 포함하고 있다. 프라이버시 쉴드 체제 하에서도 미국의 공공기관은 국가 안보나 법집행 등 공익에 필요한 한도에서 개인정보에 접근할 수 있는데, 이와 관련하여 '옴부즈만(Ombudsperson)' 메커니즘이라는 특별한 수단을 도입하였다. 미 국무부의 고위급 관료가 옴부즈만으로 지정되는데 미국의 정보기관으로부터 독립적으로 활동하며 진정 사건들이 제대로 조사·해결되도록 보장한다. 이를 위해 옴부즈만은 미국의 정보기관을 감독하는 다른 독립적 감독·조사 기구들과 협력하고 모든 정보를 얻게 된다. 옴부즈만은 비단 프라이버시 쉴드에만 관련된 것은 아니며 표준계약조항(SCC)이나 '구속력 있는 기업 규칙(BCRs)'과 같은 다른 방법을 기반으로 한 개인정보 이전을 포함하여 유럽

56) European Commission(2016), Guide to the EU-U.S. Privacy Shield.

연합으로부터 미국으로의 모든 형태의 상업적 이전과 관련된 불만을 처리한다.

한편, 유럽사법재판소의 슈렘스 I 판결 이후 아일랜드 개인정보 감독기관 DPC는 슈렘스에게 유럽사법재판소의 판결에 비추어 진정을 다시 제출하라고 요청하였다. 재진정에서 슈렘스는 여전히 미국이 자국으로 이전되는 개인정보에 대해 충분한 보호를 제공하지 않는다고 주장하며, 유럽연합에서 미국으로 자신의 개인정보가 이전되지 않도록 보류 혹은 금지해줄 것을 요구하였다. 현재 페이스북이 이용자의 개인정보를 미국으로 이전하는 것은 집행위원회의 2010/87 결정[57]에 따른 표준계약조항에 의해 이루어지고 있다. 따라서 슈렘스 진정의 결과는 2010/87 결정의 유효성에 달려있으므로, DPC는 유럽사법재판소의 사전 결정을 묻기 위해 고등법원에 소송을 제기하였다. 집행위원회가 프라이버시 쉴드 결정(2016/1250)을 채택한 것은 그 이후이다[58].

사전 결정을 요청하면서, 고등 법원은 유럽사법재판소에 GDPR이 (GDPR 발효 이전 개인정보보호 디렉티브 하에서의) 2010/87 결정에 따른 표준계약조항에 의한 개인정보의 이전에 적용되는지, 그러한 이전과 관련하여 GDPR에 의해 요구되는 보호의 수준은 무엇인지, 그런 상황에서 감독기관은 어떠한 의무를 지는지를 질의했다. 고등법원은 또한 2010/87 결정(표준계약조항) 및 2016/1250 결정(프라이버시 쉴드)의 유효성에 대해서도 문제를 제기했다.

이에 따라 유럽사법재판소는 2020년 7월 16일 내린 판결[59]에서, 기본권 헌장에 비추어 2010/87 결정을 검토한 결과 유효성에 영향을 미칠만한 것이 아무것도 없다고 판시하였다. 그러나 2016/1250 결정, 즉 프라이버시 쉴드 협정은 무효라고 선언하였다.

유럽사법재판소에 따르면, 제3국으로 이전된 개인정보가 제3국의 관할 당국에 의해 공공안전, 국방, 국가안보 등의 목적으로 처리될 수 있다고 하더라도, 그러한 방식의 개인정보 처리에 GDPR의 적용이 배제되는 것은 아니다. GDPR이 규정하고 있는 요구 조건은

57) 2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

58) 슈렘스 II 진행결과 및 판결의 주요 내용은 유럽사법재판소 보도자료 Court of Justice of the European Union(2016), PRESS RELEASE No 91/20, The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield 참조.

59) Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.

표준계약조항에 따라 제3국으로 이전된 개인정보에 대해 유럽연합 내에서 보장되는 것과 사실상 동등한 수준의 보호가 제공되어야 하는 것으로 해석되어야 한다. 그러한 보호 수준에 대한 평가는 개인정보를 이전하는 자와 이전받는 자 사이에 체결된 계약 조항뿐만 아니라, 이전된 개인정보에 대한 제3국의 공공 당국의 접근과 관련된, 제3국의 법적 시스템의 관련 측면도 고려해야만 한다. 개인정보 이전과 관련한 감독기관의 의무와 관련하여는, 집행위원회의 유효한 적정성 결정이 없을 경우, 감독기관은 모든 상황에 비추어 보았을 때 표준계약조항이 제3국에서 적용되지 않고, 다른 방법으로는 이전된 개인정보의 보호가 유럽연합 법률에서 요구하는 수준으로 보장될 수 없으며, 개인정보를 이전한 자가 스스로 그 이전을 유예하거나 중지하지 않는다고 판단할 경우 개인정보 이전을 유예 혹은 금지할 필요가 있다고 보았다.

표준계약조항과 관련된 2010/87 결정의 유효성과 관련하여 유럽사법재판소는 표준계약조항이 그 속성상 계약임을 고려할 때, 개인정보가 이전된 제3국의 관할 당국을 구속하지는 않는다는 사실만으로 이 결정의 유효성이 의문시되지는 않는다고 보았다. 하지만 그 결정이 유럽연합의 법에서 요구하는 수준의 보호를 사실상 보장하도록 하는 효과적인 메커니즘을 포함하고 있는지 여부, 표준계약조항을 위반하거나 혹은 준수할 수 없을 경우 개인정보의 이전이 유예 혹은 금지되는지 여부에 그 유효성이 달려있다고 보았다. 유럽사법재판소는 2010/87 결정이 이러한 메커니즘을 가지고 있다고 보았다. 이와 관련하여 유럽사법재판소는 이 결정이 개인정보를 이전하는 자 및 수령자에게 개인정보를 이전하기 전에 제3국에서 적절한 수준의 보호가 제공되고 있는지를 검증할 의무를 부과하고 있으며, 표준계약조항을 준수할 수 없을 경우 수령자가 이 사실을 제공자에게 고지할 것, 그리고 제공자는 개인정보 이전을 중단하고 수령자와의 계약을 종료할 의무를 부과한다고 지적하였다.

마지막으로 유럽사법재판소는 GDPR 요구 조건에 비추어 2016/1250 결정(프라이버시 쉴드 협정)의 유효성을 검토하였는데, 이 결정은 2000/520 결정(세이프하버 협정)과 마찬가지로 미국의 국가안보, 공익, 법집행 요구 조건이 우선 하며, 미국으로 이전된 개인정보 주체의 기본권 침해를 용납하는 입장을 취하고 있다고 보았다. 유럽사법재판소는 국가안보를 목적으로 미 당국의 개인정보 접근을 가능하게 하는 법률의 제도적 보호조치 및 정보 접근과 관련하여 정보주체에게 명확한 정보 제공 등의 권리 보장이 필요한데,

미 당국의 정보 접근 및 감시 프로그램을 감독하는 옴부즈만 제도가 GDPR 58(2)조에 비례한 독립성을 보장하고 있지 못하며, 미 당국을 대상으로 유럽연합의 정보주체가 제기할 수 있는 권리 이행 방안이나 법적 구제 방안이 미흡하다고 판결하였다. 특히, 미국의 외국정보감시법(Foreign Intelligence Surveillance Act, FISA) 제702조8 및 대통령 정책 지침 28조9 등 미 당국의 개인정보 접근과 관련된 법률이 정보주체의 실질적 권리 이행 및 개인정보의 적정한 보호 수준을 갖추지 못하고 있다고 보았다. 이러한 근거에서 유럽사법재판소는 2016/1250 결정이 무효라고 선언하였다[60].

과거 세이프하버 협정이 무효화 되었을 때는 당시 미국와 유럽의 당국이 몇 달 동안 이미 협상을 진행하고 있었다. 그러나 이번 판결은 행정적인 조치뿐만 아니라 입법적인 조치가 필요할 수 있어, 보다 면밀한 평가가 필요하다고 한다. 전문가들은 프라이버시 쉴드를 대체할 수 있는 협의안이 2020년 11월 미국 대선 전에 나오기는 힘들 것이라고 한다. 따라서 유럽사법재판소의 판결로 프라이버시 쉴드에 의존하여 유럽 시민의 개인정보를 미국으로 이전했던 기업들은 다른 대안을 찾을 필요가 있다. 예를 들어, 표준계약조항(SCC)이나 구속력 있는 기업규칙(BCRs) 등이 하나의 대안이 될 수 있을 것이다.[61]

2) 개인정보의 정의 : IP 주소의 사례

어디까지 개인정보로 볼 수 있을까. 개인정보의 개념 혹은 범위는 한국에서도 논란이 되고 있는 쟁점이다. 2016년 10월 19일, 유럽사법재판소는 IP 주소, 특히 인터넷에 연결할 때마다 매번 변화하는 유동 IP 주소가 개인정보인가 여부에 대한 판결을 내렸다[62]. 이용자의 ISP만이 유동 IP주소를 통해 이용자를 식별할 수 있지만, 유럽사법재판소는 온라인 미디어 서비스가 어떤 사람이 웹사이트에 접속할 때 동적 IP 주소를 등록할 경우 이를 개인정보로 보았다. 유럽사법재판소는 어떤 정보가 개인정보가 되기 위해서 "정보주체의 식별을 위한 모든 정보가 한 사람의 손에 있어야 하는 것은 아니다" 라고 하였다. ISP가 이용자를 식별할 수 있는 추가정보를 보유하고 있으므로, 유동 IP주소의 이용

60) 한국인터넷진흥원(2019), 유럽사법재판소의 프라이버시 쉴드 무효 판결 분석.
61) IAPP, Elisabeth Dehareng, Brian Hengesbaugh, 2020.7.28., "7 predictions for the road ahead after 'Schrems II", <https://iapp.org/news/a/seven-predictions-for-the-road-ahead-after-schrems-ii/>.
62) Patrick Breyer v. Bundesrepublik Deutschland(2016), C-582/14.

자는 어떤 경우, 예를 들어 사이버 공격에 따른 형사절차 과정에서 식별될 수 있다. 유럽사법재판소는 ISP가 "그 사람에 대한 추가 정보를 가지고 정보주체를 식별할 수 있는 법적인 수단을 가지고 있다면", 이는 "정보주체를 식별하는데 합리적으로 사용될 가능성이 있는 수단"을 구성하며, 따라서 그러한 데이터는 개인정보다라고 보았다[63].

3) 잊힐 권리와 검색엔진의 의무

가) 구글 스페인 판결 : 유럽사법재판소의 잊힐 권리 인정

2014년 5월 13일, 유럽사법재판소는 구글이 검색 결과 목록에서 한 이용자의 경제적 어려움에 대한 오래된 정보를 삭제할 의무가 있는지에 대한 판결[64]에서 그러한 의무를 인정하였다. 신청인의 이름으로 검색했을 때, 검색 결과는 그의 파산과 관련된 예전 기사 링크를 보여주었고, 신청인은 이를 사생활 존중 및 개인정보 보호 권리의 침해로 간주했다. 반면 구글은 자신의 책임에 이의를 제기하며 자신은 정보를 담고 있는 웹페이지에 대한 하이퍼링크를 제공할 뿐이며, 정보를 지워달라는 요청은 구글이 아니라 웹페이지의 운영자에게 해야 한다고 주장했다.

그러나 유럽사법재판소는 구글이 정보를 찾아 웹을 검색(크롤링)하고 검색 결과 제공을 위해 콘텐츠를 인덱싱할 때, 유럽연합 법 하에서 책임과 의무를 가진 컨트롤러가 된다고 보았다. 유럽사법재판소는 "정보주체의 효과적이고 완전한 보호"를 보장하기 위해서는 '컨트롤러' 개념을 넓게 정의해야 한다고 보았다. 검색엔진 운영자가 활동의 목적과 방법을 결정하고, 웹사이트 출판자에 의해 인터넷에 올려진 데이터에 이용자가 접근 가능하게 한다는 점에서 구글을 컨트롤러로 보았다[65].

또한 검색엔진 운영자의 활동도 개인정보의 '처리'이다. 유럽사법재판소는 "인터넷을 자동적으로, 지속적으로 그리고 체계적으로 정보를 찾아 탐색하면서, 검색엔진 운영자는 자신의 인덱싱 프로그램 체제 내에서 수집, 검색, 기록, 조직하고, 서버에 저장하고, 검색 결과 목록의 형태로 이용자에게 공개하고 접근 가능하도록 한다"고 말하며, "검

63) FRA(2018a) pp91-92.
64) Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD, 2014), C-131/12, Mario Costeja González [GC].
65) FRA(2018a) p105.

색 엔진 운영자가 같은 작업을 다른 형태의 정보에 대해서도 수행하고, 개인정보와 아닌 것을 구분하지 않는다는 사실에도 불구하고" 그러한 활동도 '처리'라고 결론지었다[66].

유럽사법재판소는 인터넷 검색엔진 및 개인정보를 제공하는 검색 결과는 개인에 대한 상세한 프로파일을 구축한다는 것을 명확히 했다. 디지털화가 진행될수록 개인정보가 정확해야 하고 그 공개가 필요한 이상이어서는 안 된다는 요구 조건은 높은 수준의 개인정보 보호를 보장하기 위해 필수적이다. 법적 보장이 완전한 효력을 갖기 위해서는 "그 처리와 관련된 컨트롤러는 자신의 책임, 권한, 능력 체제 내에서, 그 처리가 (유럽연합 법의) 요구조건을 충족하도록 보장해야 한다." 이는 그 처리가 더이상 필요하지 않거나 시기가 지난 것(outdated)일 때 검색엔진에도 정보주체의 삭제권이 적용된다는 것을 의미한다.

검색 결과는 개인 사생활의 다양한 측면과 관련될 수 있으며, 검색엔진이 없었다면 쉽게 상호 연결되지 않았을 것이다. 따라서 정보주체의 프라이버시권과 개인정보 권리에 대한 심각한 침해를 구성한다. 유럽사법재판소는 검색엔진에 의해 그러한 침해가 정당화될 수 있는지 검토했는데, 검색엔진 업체의 경제적 이익과 관련하여 "단지 경제적 이익만으로 그러한 침해가 정당화될 수 없음은 명백하다." 일반적으로 유럽연합 기본권 헌장 7조 및 8조의 기본권이 경제적 이익, 그리고 정보주체의 이름과 관련된 검색 정보를 찾는 일반 대중의 이익보다 우선한다고 보았다[67].

또한 유럽사법재판소는 구글이 신청인과 관련된 링크를 삭제해야 할 의무가 있는지 검토하면서 일정한 조건 하에서 개인은 자신의 개인정보가 인터넷 검색 결과로부터 삭제될 권리를 갖는다고 보았다. 이는 자신에 대한 정보가 부정확, 부적절하거나 관련이 없거나 처리 목적에 비해 과도할 경우에 발동된다. 이러한 권리가 절대적이라는 것은 아니다. 이 권리는 다른 권리, 특히 정보에 접근할 일반 공중의 권리 및 이익과의 균형이 필요하다. 따라서 개별적인 삭제 요청에 대해 사례별로 삭제 여부를 판단할 필요가 있다. 유럽사법재판소는 그러한 균형을 위해 고려해야 할 요인들에 대한 지침도 제공하고 있는데, 문제가 되는 정보의 성격이 특히 중요한 요인이 된다. 민감한 정보라면, 그리고 그

66) FRA(2018a) p99.
67) FRA(2018a) p78.

정보 접근에 대한 공공의 이익이 없다면, 개인정보 보호와 프라이버시가 더 중요하다. 이 판결 이후 29조 작업반은 유럽사법재판소 판결 이행을 위한 가이드라인을 채택했다[68]. 이 가이드라인은 개인의 삭제 요청과 관련된 진정을 다룰 때 감독기관이 사용할 수 있는, 그리고 권리 사이의 균형을 맞추기 위한 공통의 기준 목록을 포함한다[69].

잊힐 권리에 대한 유럽사법재판소의 판결은 개인정보 보호와 표현의 자유를 둘러싼 전 세계적인 논란을 촉발시켰다[70]. 검색엔진 검색 결과의 링크를 삭제하는 것은 콘텐츠 원본을 제거하는 것은 아니지만, 특정 콘텐츠를 온라인에서 발견하는 것을 어렵게 하기 때문에 표현의 자유, 정보의 자유 권리에 영향을 미친다. 물론 검색엔진 사업자가 요청을 무조건 수용해야 하는 것은 아니지만, 공익을 어떻게 해석해야 하고 그 기준은 무엇인지 모호할 수 있기 때문이다. 2019년에는 잊힐 권리와 관련된 유럽사법재판소의 판결 두 개가 나왔다.

나) GC et al v. CNIL : 구글이 삭제 요청을 무조건 수용해야 하는 것은 아님[71]

2019년 9월 24일 내려진 이 판결[72]은 검색엔진 이용자의 민감정보와 관련된 콘텐츠 링크의 삭제 요청(잊힐 권리의 행사)을 언제든 수용해야 하는가에 대한 것이다. 이 사안은 구글에게 자신과 관련된 정보의 삭제 요청을 한 4명의 개인이 관련된 것이다. 지역 정치인에 대한 풍자적인 합성 사진, 어떤 사람을 사이언톨로지 교회의 대외관계 담당으로 기술한 기사, 사업가 및 정치적 인물에 대한 사법 조사, 특정인의 아동 성폭력 형사 기소에 대한 기사 등이다. 구글은 공익상 중요한 내용이라는 이유로 이들의 요청을 거절했고, 프랑스의 감독기관인 CNIL도 구글의 결정을 지지하였다. 원고들은 이 사안을 프랑스 주법원(Conseil d' Etat)에 제소했고 주법원은 유럽사법재판소에 관련된 법의 해석을 질의했다.

---

68) ARTICLE 29 DATA PROTECTION WORKING PARTY(2014b), Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12, WP 225.

69) FRA(2018a) pp56-57.

70) Access Now(2016), ACCESS NOW POSITION PAPER: UNDERSTANDING THE "RIGHT TO BE FORGOTTEN" GLOBALLY.

71) 아래 내용은 Access Now(2019), EU Court decides on two major "right to be forgotten" cases: there are no winners here 에서 참조함.

72) GC and Others v Commission nationale de l'informatique et des libertés(CNIL, 2019), C-136/17.

유럽사법재판소는 구글 스페인 판결에서와 마찬가지로, 검색엔진 역시 컨트롤러로서 민감정보(개인정보보호 디렉티브 제8조, GDPR 제9조에서 규정하고 있는 특별 범주의 개인정보)의 처리에 대해 책임을 진다고 보았다. 그런데 구글은 민감정보를 처리하기 전에 이용자의 동의를 얻어야 하지만, 검색엔진이 모든 검색 결과에 대해 사전에 동의를 얻는 것은 불가능하다. 따라서 이용자가 먼저 구글에 자신이 동의하지 않는 개인정보가 검색 결과에 나오지 않도록 정보를 제공할 필요가 있으며, 그 이후에야 검색엔진은 조치를 취할 것이 요구된다. 또한 유럽사법재판소는 시간 경과에 따른 잊힐 권리의 적용 범위와 관련하여, 검색 엔진은 정보주체의 기본권과 일반 대중의 정보 자유의 균형을 맞추어야 한다는 의견을 제시하였다. 이때 문제가 되는 정보의 성격이나 정보주체의 사생활에 미치는 민감성과 정보에 접근할 일반 대중의 이익을 고려해야 하는데, 이는 공적 영역에서 정보주체의 지위에 따라 달라질 것이다. 이러한 유럽사법재판소의 판결에 대해 국제정보인권단체인 엑세스 나우(Access Now)는 이용자의 기본권과 공익의 미묘한 균형을 찾는 판단에 대한 책임을 사기업인 검색엔진에 맡기는 것은 큰 문제라고 지적하고 있다.

다) CNIL v. Google : 잊힐 권리의 효력은 유럽 내에 제한됨

또 하나의 판결[73]은 잊힐 권리의 효력이 미치는 범위에 대한 것이다. 2015년 CNIL은 구글이 전 세계적으로 잊힐 권리를 적용하지 않는 것에 대해 10만 유로의 과징금을 부과하였다. 즉, google.com을 비롯한 모든 도메인에 잊힐 권리가 적용되어야 한다는 것이다. 이에 대해 구글은 해당 명령의 권한은 단지 google.fr에만 적용된다고 주장하였다. 이에 대해 유럽사법재판소는 잊힐 권리는 모든 유럽의 도메인 영역에 적용된다고 판결하였다. 즉, google.fr뿐만 아니라 google.it, google.de 등 구글의 다른 유럽연합 국가 도메인에도 적용이 된다는 것이다. 유럽사법재판소는 GDPR의 채택은 유럽 전역에 걸쳐서 일관되고 조화로운 보호 수준을 요구한다는 사실을 지적하였다. 그러나 유럽연합 법 하에서 잊힐 권리를 유럽연합 역 외에도 적용해야 할 의무는 없다.

---

73) Google Inc v Commision nationale de l'informatique et des libertés (CNIL, 2019), C-507/17.

4) 감독기관의 독립성 관련 판결

유럽사법재판소는 여러 판결을 통해 개인정보 감독기관의 '완전한 독립성'의 의미를 구체화하였다.

2010년 유럽사법재판소는 독일 개인정보 감독기관에 대한 판결[74]에서 개인정보 감독기관들이 지침에서 보장된 개인정보 처리와 관련된 권리의 '수호자' 이며, 완전히 독립적인 감독기관의 설치는 "개인정보의 처리와 관련하여 개인을 보호하기 위한 필수적인 구성요소" 라고 강조하였다. 유럽사법재판소는 독일 각 주에서 주 정부가 민간 부문을 감독하는 개인정보 감독기관을 통제하는 것이 '완전한 독립성' 에 반하는 것이라고 판단하였는데, 개인정보 감독기관이 '완전한 독립성' 을 가지고 기능하는 것에 대한 법적 요건은 피감독 기관들로부터의 영향만이 아니라 국가나 주의 직접 또는 간접적인 영향을 포함하여, 어떠한 외부의 영향력으로부터도 자유로운 의사결정 권한을 의미한다고 보았다[75].

2012년 유럽사법재판소는 오스트리아 개인정보 감독기관인 정보보호위원회(DSK)가 개인정보보호 디렉티브 제28조의 완전한 독립성 의무를 이행하지 않고 있다고 판단하였다[76]. 오스트리아의 개인정보 보호법이 DSK에 대해 운영상 자율성을 규정하고 있음에도 불구하고, 그 상임위원 및 사무처의 직제에 있어서 완전히 독립적이지 않았기 때문이다[77].

2014년 헝가리에 대한 판결[78]에서도 유럽사법재판소는 개인정보 감독기관의 완전한 독립성 요건을 확인하였다. 이 사건에서는 정부가 개인정보 감독기관의 재직기간을 조기에 종결시킨 것이 문제가 되었는데, 유럽사법재판소는 완전한 독립성의 보장은 "기관이 전 임기를 재직하는 것을 허용할 의무를 수반" 한다고 판시하였다[79].

---

74) European Commission v. Federal Republic of Germany [GC](2010), C-518/07.
75) 이은우 외(2018), 앞의 글, p21.
76) European Commission v. Republic of Austria(2012), C-614/10.
77) 이은우 외(2018), 앞의 글, p22.
78) European Commission v. Hungary(2014), C-288/12.
79) 이은우 외(2018), 앞의 글, pp22-23.

2. 미국

가. 미국의 개인정보 보호 법제

미국은 공공 및 민간부문을 포괄하는 종합적인 개인정보 보호법을 가지고 있지 않다. 공공부분에서는 연방 차원의 1974년 프라이버시법(Federal Privacy Act of 1974)이 있으며, 각 주(州)에서도 프라이버시 보호 관련 법률을 갖고 있다. 민간 부문에서는 원칙적으로 시장 자율규제에 맡기고 다만, 연방정부가 개입해야 할 필요가 있는 특정 영역, 예컨대, 공공, 금융, 통신, 교육, 의료, 비디오 감시, 근로자 정보 등의 영역에 대하여 영역별로 접근하는 방식을 택하고 있다[80].

미국은 유럽연합 등 다른 나라에 비해 상대적으로 빅데이터의 활용에 유리한 법적 환경을 가지고 있는 것으로 통상적으로 평가받고 있지만, 오바마 정부 하에서 미국 역시 빅데이터 등 변화하는 정보통신환경에 대응하여 개인정보 보호를 강화하는 움직임을 보여 왔다.

2010년 3월 26일, 미 연방거래위원회(FTC)는 인터넷 사용자들의 프라이버시 보호를 위해 〈급속한 변화의 시대의 소비자 개인 정보 보호〉 보고서[81]를 발간하였는데, 이 보고서는 기업들과 정책 결정자를 위한 권고안으로 추적 금지(Do-Not-Track) 옵션의 제공, 설계에 의한 프라이버시 보호(Privacy by Design), 데이터 브로커에 대한 규제 등의 내용을 담고 있다.

2012년 2월 23일, 오바마 정부는 디지털 경제의 성장을 도모하면서도 동시에 소비자의 프라이버시 보호 개선을 위한 전면적 청사진으로 '온라인 프라이버시의 프레임워크'[82]을 발표하였다. 이 프레임워크는 '소비자 프라이버시 권리장전(Consumer Privacy bill of Rights)'을 포함하고 있는데, 이는 1970년대 이래 사실상 '모델 프라이버시법'으로 역할을 해온 '공정 정보 관행 규약(Code of Fair Information Practices, FIPPs)'을 최근의 IT 환경에 적합하도록 대폭 보완한 것이다[83]. 소비자 프라이버시 권리장전은 ▲ 자기정

80) 이상경, 남정아(2017), 미국의 개인정보 보호법제 연구, 2017년 개인정보보호위원회 연구용역보고서. p1
81) FTC(2012), Protecting Consumer Privacy in an Era of Rapid Change.
82) White House(2012), Consumer Data Privacy in a Netwokred World - A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.
83) 이상경, 남정아(2017), 앞의 글, p48

보 통제권(Individual Control), ▲ 투명성(Transparency), ▲ 맥락의 존중(Respect for Context), ▲ 정보보안(Security), ▲ 접근성 및 정확성 강화(Access and Accuracy), ▲ 최소수집의 원칙(Focused Collection), ▲ 책임성 강화(Accountability) 등 7개의 원칙을 제시하고 있다.

그러나 이러한 오바마 행정부의 개인정보 보호 강화 정책은 트럼프 행정부 내에서 이어지지 못했다. 예를 들어, 인터넷 사용자의 개인정보 보호를 위해, 2016년 FCC가 제정한 '광대역 및 기타 통신·서비스 고객의 개인정보 보호에 관한 FCC 규칙'은 2017년 12월 시행 예정이었지만, 2017년 4월 트럼프 정부의 의회에서 폐기되었다[84].

나. 캘리포니아 소비자 프라이버시 보호법 (CCPA)[85]

2018년 6월 28일 캘리포니아 주에서 '캘리포니아주 소비자 프라이버시 보호법(The California Consumer Privacy Act of 2018, CCPA)'이 채택되었다. 주민의 개인정보 보호권 증진을 위해 기존의 법을 보충하고자 하는 목적이었으며, 2020년 1월 1일부터 시행되었다. 캘리포니아주 헌법은 이미 1972년에 주민투표를 통해 모든 사람의 양도할 수 없는 권리로서의 '프라이버시권'을 신설했으며 이후 온라인 프라이버시법, 디지털 캘리포니아 미성년자 프라이버시 권리법 등을 제정한 바 있다. CCPA는 주민발안 법안[86]으로 시작되었고, 주민발안 법안을 철회시키려고 제안한 의원발의안이 통과된 것이다.

CCPA에는 ① 어떠한 개인정보가 수집되고 있는지 알 수 있는 권리 ② 개인정보가 판매, 공개되는지 여부와 누구에게 판매, 공개되는지를 알 수 있는 권리 ③ 개인정보 판매에 대해 거부할 수 있는 권리 ④ 자신의 개인정보에 접근할 수 있는 권리 ⑤ 개인정보 보호 권리를 행사해도 동일한 서비스와 가격을 누릴 수 있는 권리가 포함되어 있다.

또한 CCPA는 개인정보에 대한 정의 개념을 확대해 '특정 소비자나 가구(household)를 식별하고 묘사하거나, 관련 있거나 관련될 수 있거나, 직접 또는 간접적으로 합리적

84) 이광석 외(2018), 앞의 글, pp123-124.
85) California legislative information, 2018.06.29., "CCPA", <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375>
86) 주민발안 법안에 대해서는 <https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf> 참고.

으로 연결될 수 있는 정보’로 정의했다. 예를 들어 개인의 구매내역 등을 포함하는 상업정보・바이오정보・검색기록・교육정보・소비자의 선호도를 반영하는 프로파일을 생성하기 위해 식별정보로부터 도출된 추론사항 등이 포함된다. 이 ‘개인정보’에는 공개적으로 이용 가능한 정보는 포함되지 않는데, ‘공개적으로 이용 가능’하다는 의미는 해당 정보와 관련된 조건이 있는 경우에는 연방, 주, 지방 정부 기록에서 합법적으로 이용할 수 있다는 것을 말한다.[87]

CCPA는 비식별 정보의 개념과 가명처리의 개념을 모두 포함하고 있다. 비식별 정보는 ‘특정 소비자를 합리적으로 확인할 수 없거나 이를 관련시켜 설명하거나 직접 또는 간접적으로 연관되거나 연결될 수 없는 정보’로 정의된다. 사업자는 재식별을 금지하는 기술적 안전조치를 이행해야 하며 재식별을 구체적으로 금지하고 시도하지 않을 의무가 있다. 가명처리는 ‘추가적인 정보를 사용하지 않고서는 식별되지 않도록 개인정보를 리하는 것’을 의미하며, 이러한 추가정보는 별도로 보관되고 기술적・관리적 조치를 거쳐야 한다.

CCPA는 소비자의 옵트인과 옵트아웃 권리도 명시하고 있다. 여기서 소비자는 ‘캘리포니아 주민인 자연인으로서 고유한 식별자에 의해서 식별된 자’를 의미한다[88]. 고유한 식별자에 대해서는 ‘시간이 지남에 따라서 다양한 서비스를 통해서 특정 소비자, 가족 또는 소비자나 가족과 연관되는 기기를 인식하기 위해서 사용될 수 있는 영구 식별자’로 규정되어 있다.

옵트아웃 권리를 행사한 소비자나 미성년자의 개인정보의 경우, 승인을 받지 않는 한 판매가 금지된다. 소비자가 제3자의 개인정보 판매에 대해 명백한 고지를 받지 못하거나 옵트아웃을 행사할 권리를 얻지 못하면 제3자는 사업자로부터 구매한 소비자의 개인정보를 판매할 수 없다. 또한 옵트아웃 권리 고지는 눈에 띄게 제공해야 한다.

이외 소비자의 개인정보를 삭제하도록 사업자에게 요구할 수 있는 권리 등이 규정되어 있으며, 소비자가 상기 권리를 행사했다고 해서 사업자가 해당 소비자를 차별해선 안된다는 규정도 명시되어 있다. 또한 사업자는 상기 규정을 준수하기 위해 수집・판매・공개했던 개인정보 범주 목록을 공개하고 1년마다 한 번씩 업데이트해야 하며, 소비자가

87) 한국인터넷진흥원(2018), 미국 캘리포니아 주「소비자 프라이버시법」(The California Consumer Privacy Act of 2018) 주요내용 분석, p160.
88) 캘리포니아주 법령 18편 17014조 정의조항 참조.

확인 요구를 할 경우 45일 이내에 필요한 정보를 무료로 공개 및 제공해야 한다.

이렇듯 CCPA는 GDPR과 흡사하게 개인정보 보호에 대한 광범위한 내용을 규정하고 있다. 또한 입증된 소비자 피해가 없더라도 잠재적으로 상당한 벌칙이 기업에 부과될 수 있도록 하고 있고, 캘리포니아 주 법무장관에게 광범위한 집행 권한을 부여하고 있다. CCPA는 주법이기에 캘리포니아 주에서 사업을 하는 일정 조건의 영리 기업에게만 적용된다는 한계가 있다. 그러나 소비자 프라이버시 보호라는 관점에서 제정된 개인정보 보호 법제라는 점, 주민의 제안에서 발의가 시작되었다는 점에서 큰 의의가 있다.

다. CCPA 통과 이후 미국의 개인정보 보호 법제 입법 흐름

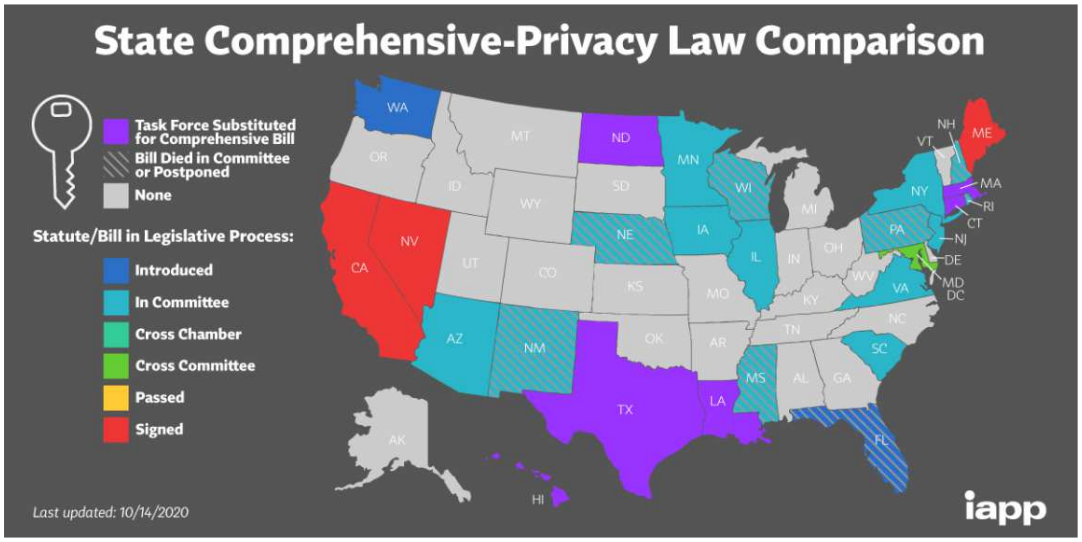
2018년 5월 GDPR이 발효됨에 따라 미국 기업도 그 영향권에 놓였고, 같은 해 6월 미국 주 정부로서는 처음으로 캘리포니아에서 CCPA가 채택되면서 미국에서도 포괄적인 개인정보 보호 법제의 입법 필요성이 대두되었다[89].

CCPA 통과 이후, 다수의 다른 주에서도 포괄적인 개인정보 보호법이 제안되거나 통과하고 있는데, 네바다 주에서 통과한 '인터넷 프라이버시법'은 CCPA보다 이른 2019년 10월 발효[90]하였고, 메인 주는 2020년 7월 1일, 인터넷서비스제공자가 수집하는 소비자 정보에 초점을 둔 온라인 소비자정보 프라이버시 보호법을 통과시켰다.[91] 국제 프라이버시 전문가협회의 서부연구센터는 미국 전역에 걸쳐 제안된 포괄적인 프라이버시법의 목록 및 비교표, 그리고 입법 현황을 업데이트하고 있다[92].

연방 차원에서도 포괄적인 프라이버시법이 제안되고 있는데, 미국 상원의원에서 2019년에만 「소비자 온라인 프라이버시권 법(Consumer Online Privacy Rights Act)」(마리아 캔트웰Maria Cantwell), 「2019년 온라인 프라이버시권 법(Online Privacy Act of 2019)」(안나 에슈Anna G. Eshoo), 「프라이버시 권리장전 법(Privacy Bill of Rights Act)」(에드

89) 이규엽 외(2020), 미국 개인정보보호법 입법 동향: 국내 개정법과의 비교 및 시사점, p4.
90) 네바다 주 인터넷 프라이버시법에 대해서는 <https://legiscan.com/NV/text/SB220/2019> 참조.
91) 메인 주의 온라인소비자정보프라이버시보호법에 대해서는 <http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=SP0275&item=9&snum=129> 참조.
92) IAPP, "US State Comprehensive Privacy Law Comparison", <https://iapp.org/resources/article/state-comparison-table/>.

<그림2-6> 미국 각 주의 포괄적인 프라이버시법 비교



* 출처: IAPP

마키Edward Markey), 「데이터 프라이버시 법(DATA Privacy Act)」(캐서린 코테즈 매스토Catherine Cortez Masto) 등 4건의 입법안이 제안되었다.

이 중 민주당 마리아 캔트웰 상원의원의 「소비자 온라인 프라이버시권 법」(안)과 공화당 안나 에슈 상원의원의 「2019년 온라인 프라이버시권 법」(안)을 상호 비교해 보면, 두 법안은 공통적으로 접근권, 삭제권, 정정권, 이동권 등을 개인의 권리로 보장하는 내용을 담고 있다[93]. 또한 두 법안 모두 알고리즘과 자동화된 의사결정과 관련된 권리 및 의무를 규정하고 있으며, 기업의 의무로 필요 최소한의 데이터 처리 및 유지 의무, 위험평가 의무 등을 포함하고 있다.

두 법안의 가장 큰 차이점은 비식별 정보의 개념에 있다. 민주당의 「소비자 온라인 프라이버시권 법」(안)은 적용 대상에 대해 '개인 또는 소비자 전자기기를 식별 또는 연결하는(또는 합리적으로 연결 가능한) 정보'라고 정의하면서 비식별 정보는 제외하고 있다. 반면 공화당의 「2019년 온라인 프라이버시권 법」(안)은 적용 대상에 대한 정의 규정 없이 공개 행위에 대한 정의에서 '개인정보 및 통신 내용과 관련이 있다'고 정의할 뿐이며, 특히 개인정보에 대한 정의에서 비식별 정보가 개인정보에 포함된다고 규

93) 이규엽 외(2020), 위의 글, pp5-6.

정하고 있다. 또한 알고리즘과 관련하여 「소비자 온라인 프라이버시권 법」(안)은 알고리즘 의사결정에 관한 정의는 물론 알고리즘 공정성 등에 대한 적용대상 주체의 설명 및 평가 의무를 규정하고 있는 반면, 「2019년 온라인 프라이버시권 법」(안)은 알고리즘 대신 '자동화된 의사결정 과정'이라는 용어를 사용하면서도 정의 규정은 두지 않고 인간에 의한 재검토를 요구할 권리까지 보장한 것에 차이가 있다.

한편, 미국의 정보인권 시민단체들도 포괄적인 프라이버시법 제정을 촉구하는 활동을 전개하고 있다. 미국의 정보인권 단체인 전자프라이버시정보센터(EPIC)는 미국에도 개인정보 감독기관이 절실하게 필요하다며 캠페인을 벌이고 있다.[94] EPIC은 미국이 개인정보 감독기관이 없는 유일한 OECD 국가라고 비판한다. 유럽의 시민들은 열람권, 삭제권, 이동권, 개인정보 유출시 고지 받을 권리 등을 보장받고 있지만, 미국의 시민들은 그러한 권리를 보장받고 있지 못하고, 미국의 기술 기업들도 유럽 시민의 개인정보는 보호할 의무가 있지만, 미국의 시민에 대해서는 그러한 의무가 없다는 것이다. 연방거래위원회(FTC)가 있지만 시장에서 불공정하고 기만적인 관행에 대한 집행 권한만 있을 뿐 온전한 개인정보 감독기관이라고 할 수 없다. 미국의 또 다른 정보인권 단체인 민주주의와기술센터(CDT)는 지난 2018년 12월, 아예 연방차원의 프라이버시법을 위한 토론용 초안을 제안하였다. 이 초안은 개인정보의 이용, 수집, 공유에 대한 합리적인 제한 및 정보주체의 접근, 정정, 이동권 등을 담고 있다[95].

3. 일본

가. 일본의 개인정보 보호 법제 개요

일본의 개인정보 보호법은 2003년 5월에 제정되었다. 일본의 개인정보 보호법은 사회 전반의 개인정보 보호의 기본이념 등을 정한 기본법이면서, 민간사업자가 지켜야 할 의무 등을 정하고 있다. 개인정보 보호법 제정과 동시에 공공부문에도 함께 적용되는 '행정기관의 개인정보 보호법', '독립행정법인의 개인정보 보호법', '정보공개・개인정보보호 심사회 설치법', '행정기관이 보유하는 개인정보의 보호에 관한 법률 등의 시

94) EPIC의 개인정보 감독기구 개설 캠페인 페이지, <https://www.epic.org/dpa/>.
95) CDT의 초안은 <https://cdt.org/collections/federal-privacy-legislation/> 참조.

행에 따른 관계 법률의 정비 등에 관한 법률’ 의 4개 관련법이 같이 정비되었다. 아울러 개인정보 보호법이 제정되기 전 원래 존재했던 자치단체의 ‘개인정보 보호 조례’와 관련해 의료, 금융, 정보통신 분야 등의 가이드라인 등도 제・개정, 시행되었다[96].

일본은 2015년에 개인정보 보호법을 개정하였는데, 개정의 중요한 이유 중 하나는 빅데이터, 인공지능 등의 기술 환경의 변화에 대응하여 개인정보를 정보주체의 동의 없이 용이하게 활용할 수 있도록 하는 것이었다. 개정 개인정보 보호법 제1조 목적 조항에 ‘개인정보의 적정하고 효과적인 활용으로 새로운 영역의 사업・서비스 창출’이란 문구가 포함된 것은 이러한 취지를 반영하고 있다. 이와 동시에 잇따른 개인정보 대량 유출 사건으로 개인정보 취급에 대한 국민들의 불안이 높아지면서 이에 대한 대책을 마련하려는 취지도 있었다. 일본의 개인정보 보호법의 개정은 유럽연합의 GDPR 시행과 발맞추어 국제적인 기준을 준수하기 위한 것이기도 했다[97].

2016년 1월, 개인정보 보호법에 근거하여 개인정보 감독기구인 개인정보 보호위원회가 설치되었다. 그리고 개인정보 보호위원회에 의해서 개인정보 보호법의 시행령, 시행규칙, 기준 등의 세부 사항 등이 만들어졌다. 개정 개인정보 보호법은 2017년 5월 30일에 전면 시행됐다.

나. 일본 개정 개인정보 보호법의 주요 내용

개정 개인정보 보호법은 기존에 개인정보 여부가 불명확했던 회색 지대를 해소하기 위해 개인정보의 정의를 명확히 하였다. 개인식별부호가 포함된 것을 개인정보 개념으로 포섭하였다. DNA와 바이오 정보는 물론 “보행 때 자세 및 양팔의 동작, 보폭 그 외 보행의 양태”도 추가하여 빅데이터에서 흔히 말하는 비정형 데이터도 개인식별부호에 포함하였다[98]. 요(要)배려 개인정보는 인종, 신조, 사회적 신분, 병력, 범죄의 경력, 범죄로 인해 피해를 입은 사실 및 그 밖에 본인에 대한 부당한 차별, 편견 및 그 밖의 불이익이 생기지 않도록 그 취급에 특별히 배려를 요하는 것으로서 정령[99]으로 정하는 기술 등이

96) 손형섭(2012), 개인정보보호법의 특징과 앞으로의 방향- 업계의 반응에 대한 몇 가지 대안을 중심으로, 언론과 법, p114.
97) 손형섭(2019), 한국 개인정보보호법과 일본 개인정보보호법의 비교 분석- ICT산업 생태계에 미치는 영향을 중심으로, 2019 NAVER Privacy White Paper, pp13-15.
98) 손형섭(2019), 위의 글, p17

포함되는 개인정보로 정의되며, 우리나라의 민감정보에 해당한다.

빅데이터, 인공지능 등 신기술 발전에 따른 데이터 활용 촉진을 위해 '익명가공정보' 개념을 도입하였다. '익명가공정보'란 특정 개인을 식별할 수 없도록 개인정보를 가공하여 얻어지는 개인에 관한 정보로서, 당해 개인정보를 복원할 수 없도록 한 것으로 정의된다. 익명가공정보는 개정 개인정보 보호법 제2조 제9항에 따른 기술적 조치를 취해야 하며, 또한 원래 데이터와 조합하여 재식별하는 행위를 하지 않는 등의 관리적 조치도 취하여야 한다. 재식별 가능성을 염두에 두고 있다는 점에서 GDPR이나 우리나라 개인정보 보호법에서 상정하고 있는 익명정보라기 보다는, 가명정보에 가깝다[100]. 이렇게 개인을 특정할 수 없도록 처리된 익명가공정보는 정보주체의 동의없이 유통 및 거래가 가능하다.

일본의 개인정보 보호법은 개인정보의 수집에 있어 옵트아웃 방식을 채택하고 있다는 점에서 우리나라의 개인정보 보호법이나 GDPR과 다르다. 즉, 이용목적을 특정하고 통지하기만 하면 그 범위 내에서 자유로이 수집·이용할 수 있다. 다만, 당초 특정한 이용목적 달성에 필요한 범위를 초과하는 경우(제16조) 및 요배려(要配慮) 개인정보(제17조 2항)를 수집할 경우에는 사전에 동의를 받아야 한다.

일본 개인정보 보호법은 개인정보의 제3자 제공의 일반적인 요건으로 '사전 동의'를 규정하고 있다. 다만, 법령에 근거한 경우, 사람의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때 등 사전 동의 예외 사유를 인정하고 있다(제23조 1항). 이와 함께, 정보주체의 동의를 받지 않고 개인정보를 제3자 제공할 수 있는 요건을 규정하고 있는데, 정보주체의 정지요구권을 보장해야 하고 개인정보 제3자 제공을 이용목적으로 한다는 점 및 그 제공 항목과 방법 등을 정보주체에게 미리 통지하거나 또는 정보주체가 용이하게 알 수 있는 상태에 두고 있으면서 개인정보 보호위원회에 신고할 것 등이다. 요(要)배려 개인정보에는 이 규정이 적용되지 않는다[101].

---

99) 내각에 의한 명령, Cabinet Order. 우리나라의 대통령령에 해당.

100) 김경환(2016), [ICT법 바로알기 73] 일본 개인정보보호법과 빅데이터 목적의 익명가공정보(1), <http://www.ddaily.co.kr/news/article.html?no=140860>

101) 전승재, 권헌영(2019), 개인정보 수집, 이용, 제3자 제공에 관한 4개국 법제 비교분석, 선진상사법률연구 통권 제85호, pp 190-191.

<표2-1> 일본 개인정보 보호법의 주요 개정 내용

개인정보 개념 명확화	- 개인의 신체적 특징을 데이터화한 정보, 운전면허증, 마이넘버 등 특정 개인을 식별가능한 정보인 개인식별부호가 포함된 정보를 개인정보로 명확화. - 요(要)배려 개인정보(민감정보)에 관한 규정 정비
데이터 활용 촉진을 위한 법・제도 구축	- 익명가공정보에 대한 가공처리 방법 및 취급 등 규정 정비, - 익명가공정보의 경우 정보주체의 동의없이 제3자 제공 가능 - 개인정보 보호 지침의 작성 및 신고, 공표 등의 규정 정비
개인정보 보호 강화	- 개인정보 취급 시 정보주체의 권리보장을 위한 동의 및 고지 절차 제정(개인정보 취급 시 옵트아웃의 신고, 공표 등 엄격화) - 개인정보 데이터베이스 등을 부정 제공할 경우의 처벌규정 신설 - 정보주체 이외로부터 수집한 경우(조합에 의한 개인정보 생성, 제3자로부터 제공받은 경우 등)에 있어 고지 절차
명부업자의 법적 지위 명확화	- 명부업자에 대해 필요에 따라 개인정보의 유통경로를 알 수 있도록 함 - 명부업자가 부정하게 개인정보를 제공한 경우의 벌칙을 신설 - 명부업자의 부정한 개인정보의 유통을 방지 - 추적가능성(traceability) 확보(제25조, 제26조 3항 및 4항): 개인정보의 제3자 제공시 수령자는 제공자의 성명 및 데이터 취급경위 등을 확인하고, 일정 기간 그 내용을 보관, 제공자도 수령자의 성명 등을 일정 기간 보존, 개인정보의 제공자, 제공처, 연월일 등 기록 작성 및 보존 의무.
개인정보 보호위원회 신설 및 권한 부여	- 내각부 외국(外局)으로 개인정보 보호위원회를 신설 - 위원장+8명 위원(4명은 비상근, 임기 5년, 전문위원) - 기존 각 산업별로 13개 성/청, 27개 분야의 주무장관이 담당하고 있던 업무・권한 일원화
번호이동법	- 특정개인정보(마이넘버)의 이용 추진에 관한 제도 개정 - 금융, 의료 등 분야에 이용범위 확대 - 예・적금계좌에의 번호, 특정검진, 보험지도에 관한 사항에 이용, 예방접종에 관한 사무에 있어서 접종이력 연대 등
개인정보 국외이전에 대한 대응	- 일본 국민의 개인정보 국외이전의 허용요건, 안전 관리규정 등 포함(데이터가 국경을 넘는 경우, 국내외 기업에 동일하게 적용)
그 외 개정 사항	- 이용목적 변경이 가능하도록 규정 완화 - 취급 개인정보가 5,000명 이하인 소규모 사업자에게도 동 법 적용(적용 범위의 확대)

* 출처: 이정은(2019), EU 일반개인정보보호법(GDPR)에 대한 일본정부의 대응 및 평가, 손형섭(2019), 앞의 글 참조.

제25조, 제26조에서는 추적가능성 관련 규정을 두고 있다. 수령자는 제공자의 성명이나 데이터 취득경위 등을 확인하고 일정기간 그 내용을 보존하며, 제공자도 수령자의 성명 등을 일정기간 보존하도록 하였다.

일본 개인정보 보호 체계에서 명부업자란 5천 건이 넘는 개인정보를 사업용으로 제공하는 개인정보 취급업자를 가리킨다. 2014년 일본에서 대규모 고객정보 유출 사태가 발생한 이후 명부업자에 대한 규제 검토가 수면 위로 떠올랐다. 개정 개인정보 보호법에서는 개인정보의 제3자 제공에 대해 사업자에게 기록 의무를 부과했으며, 이에 대해 개인정보 보호위원회에 반드시 신고하도록 가이드라인으로 지정했다[102].

또한, 일본의 개인정보 보호 정책을 총괄하는 개인정보 감독기관으로서 개인정보 보호위원회를 설립하였다. 원래는 마이넘버법에 근거하여 2014년 1월에 특정개인정보 보호위원회가 설치되어 마이넘버 관련 업무를 담당하였는데, 개인정보 보호법 개정에 따라 개인정보 보호위원회로 개편되었다. 위원회는 위원장 및 8인의 위원으로 구성되는데 4인은 비상근이다. 위원장 및 위원은 양의원(참의원, 중의원)의 동의를 얻어 내각총리대신이 임명하며, 임기는 5년이며 재임할 수 있다. 총리의 지휘감독을 받지 않고 독자적으로 권한을 행사할 수 있으며, 개인정보 보호법의 규칙 제정, 감시・감독 및 집행권을 아우르는 권한을 보유하고 있다.

다. GDPR과 일본의 상호 적정성 결정

일본은 개인정보 보호법 개정 전인 2014년 3월부터 2019년에 GDPR 적정성 인정을 받기까지 유럽연합 집행위원회와 20여 차례 회담을 통해 의견을 교환했다. GDPR이 2018년 5월에 시행된 점을 보면 협상이 이른 시점에 발 빠르게 이루어졌음을 알 수 있다. 이외에도 유럽 각국의 개인정보 감독기관을 방문해 방문국의 개인정보 보호 법제와 개인정보 감독기관에 대한 의견을 수집하기도 했다.

일본은 이와 같은 과정을 바탕으로 2018년 6월 유럽연합에서 이전되는 개인정보에 대해서만 적용되는 보조규칙을 마련했다. 이는 일본의 개정 개인정보 보호법이 GDPR에 비추어 미흡한 부분이 있었기 때문인데, 보조규칙을 통해 GDPR과 동등한 수준을 확보하고

102) 일본 개인정보위원회, “개인정보보호법에 대한 가이드라인(제3자 제공 시의 확인·기록 의무사항 편)”, <https://www.ppc.go.jp/files/pdf/guidelines03.pdf>

<표2-2> 유럽연합과의 협상 이후 일본 정부가 도입한 추가 보호조치 : 보조규칙(supplementary rules)

항목	개정 개인정보 보호법	내용
요要배려 개인정보	2조 3항	요要배려 개인정보(민감정보)의 범위 확대
		GDPR에서 특별한 유형의 개인정보(Special Categories of Personal Data)로 정의한 성적취향, 노동조합 등에 대한 정보도 요(要)배려 개인정보 취급
보유개인정보	2조 7항	보유개인정보 범위 확대(기간한정 예외조항 삭제)
		유럽연합에서 이전된 개인정보에 대해서는 '해당 정보의 존재 여부가 밝혀질 경우 공익 또는 기타 이익이 침해될 우려가 있는 경우'에 해당하지 않는 한 기간에 관계없이 보유개인정보로 취급(기존에는 6개월 이내에 삭제 예정인 개인정보는 보유개인정보로 취급하지 않았음.)
이용목적 특정	15조1항・16조1항・26조1・3항	개인정보 취득 시 이용목적을 확인・기록하여 그 범위 내에서 이용하도록 조치
		유럽연합에서 이전된 개인정보에 대해서는, 취득 시 확인한 이용목적의 범위 내로 그 목적을 제한하여, 그 범위 내에서 해당 개인정보를 이용하도록 함.
역외 제3자에게 정보 제공 제한	24조・규칙 11조의2	일본에서 유럽연합 외 제3국으로 개인정보가 재이전되는 경우의 보호수준 강화
		유럽연합에서 이전된 개인정보에 대해 본인 동의에 따라 재이전하는 경우 본인이 동의하는 데 필요한 목적지 상황에 대한 정보를 제공하고, 개인정보 보호법과 동일한 수준의 보호조치를 시행하도록 함.
익명가공정보	2조 9항・36조 1・2항	개인정보의 익명가공처리방식에 대한 정보 제거
		유럽연합에서 이전된 개인정보를 개인정보 보호법상의 익명가공처리하는 경우, 가공방법에 대한 정보를 삭제하고 재확인이 불가능하도록 조치. 유럽연합에서는 가공방법에 대한 정보가 남아 있을 경우, 안전하게 분리하여 보관할 경우에도 재식별의 가능성이 있다고 판단, 익명화되었다고 간주하지 않음.

*출처 : 이정은(2019), 앞의 글, p.8

자 한 것이다. 추가 보호조치로서 도입된 보조규칙은 요要배려 개인정보(민감정보)의 범위 확대, 보유 개인정보의 범위 확대(기간한정 예외조항 삭제), 개인정보 취득 시 이용목적을 확인 및 기록해 범위 내에서 이용하도록 하는 조치, 일본에서 유럽연합 외 제3국으로 개인정보를 재이전하는 경우 보호수준 강화, 개인정보의 익명가공처리방식에 대한 정보 제거 등[103]이다.

유럽연합과의 협상 과정에서 보조규칙 외에도 정부에서 따로 정부기관의 개인정보 접근제한 및 보호장치도 함께 도입했다. 형법 집행 및 국가안보 등의 목적으로 정부기관이 개인정보에 접근할 경우 목적 제한 등과 이를 위반할 경우의 처리기구를 개인정보 보호위원회가 관리・감독하도록 하는 등의 보호장치다.

2019년 1월 23일 일본 개인정보 보호위원회와 유럽집행위원회는 양국의 개인정보 보호체계가 동등한 수준이라고 인정하는 상호 적정성 평가를 최종적으로 승인하였다. 즉, GDPR에 따른 일본의 적정성 결정만이 아니라, 일본의 개정 개인정보 보호법에 따른 유럽연합의 적정성 결정도 상호적으로 이루어진 것이다.

우리나라의 경우에는 GDPR에 따른 적정성 평가만 이루어지고 있는데, 우리 개인정보 보호법도 적정성 결정 제도를 도입하여 상호적으로 이루어지도록 할 필요가 있다. 또한, GDPR 2년 평가 부분에서 언급한 바와 같이 EDPB는 일본과의 적정성 결정 과정에서 추가규칙이 활용된 것에 대해 의구심을 표하고 있다. 즉, 추가 규칙은 제3국의 개인정보 보호 법제가 GDPR과 일정한 간극이 있다는 것을 의미하기 때문에, 향후 그러한 추가 규칙이 구속력을 가지고 효과적으로 적용되는지 모니터링할 필요가 있다고 강조한 것이다. 이러한 점을 고려하면, 추가 규칙을 활용한 일본의 사례를 모범 사례로 볼 것이 아니라 가급적 GDPR과 동등한 수준으로 개인정보 보호 법제를 개선하는 것이 바람직할 것이다.

103) 이정은(2019), 앞의 글, p8.

제3장 국내 개인정보 보호법제의 현황과 쟁점

제1절 신기술과 개인정보를 둘러싼 사회적 논란의 경과[104)]

1. 개인정보 비식별 조치 가이드라인

빅데이터 분석 목적의 개인정보 활용에 대한 논란은 결국 '비식별 처리된 정보', 즉 '가명정보' 활용의 적법성 논란이라고 볼 수 있다. 박근혜 정부는 개인정보의 수집 목적 외 활용을 위해 가이드라인에 '비식별'이라는 법적 근거가 없는 개념을 도입해 가명정보를 일정한 조건 하에 활용할 수 있도록 했고, 이는 자연스럽게 개인정보 보호법 위반 논란을 야기했다. 법에 근거하지 않은 개념을 사용했을 뿐 아니라, 가이드라인에 따라 비식별에 대한 개념도 바뀌어 수범자의 혼란을 가중시켰다.

비식별(de-identification)이란 개인정보에서 식별자를 제거하는 것을 의미하는데 식별자를 어떻게, 얼마나 제거하느냐에 따라 그 결과는 다른 정보와 결합해도 더이상 개인을 식별할 수 없는 익명정보(anonymised data)가 될 수도 있고, 다른 정보와 결합하면 개인을 식별할 수 있는 가명정보(pseudonymised data)가 될 수도 있다.

가. 개인정보 비식별화 개념의 도입

국내에서 처음 비식별 개념이 도입된 것은 2013년 9월 발표된 <공공정보 개방·공유에 따른 개인정보 보호 지침>이다. 이 지침은 "공공정보 개방 공유 및 개인 맞춤형 서비스 확대에 따른 개인정보 침해 요소에 대한 선제적 보호조치 강화 및 안전한 활용 기반 마련"을 목적으로 만들어진 것인데, '비식별화'를 "개인정보의 일부 또는 전부를 삭제하거나 다른 정보로 대체함으로서 다른 정보와 쉽게 결합하여서도 특정 개인을 식별하기 어렵도록 하는 일련의 조치"로 규정하고 있다. 그러면서 "비식별화된 정보가 다른 정보와의 연계(매칭) 등을 통해 특정 개인을 알아볼 수 있는 개인정보가 되는 것"을 '재식별화'로 규정했는데, 이는 비식별화된 정보가 다시 재식별될 수 있음을 염두에

104) 이광석 외(2018), 앞의 글, pp160-173 참조.

둔 것이다.

당시 개인정보 보호법은 제2조 1호에서 개인정보란 “살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통해 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합해 알아볼 수 있는 것을 포함한다)를 말한다” 고 정의하였다. 따라서 비식별화된 정보 역시 다른 정보와 결합해 재식별될 수 있다면 개인정보에 해당한다. 그럼에도 불구하고 이 지침은 개인정보를 애초 수집 목적 외로 분석, 활용하려는 경우, 그 법적 근거가 없을 때에는 “비식별화 조치 후 분석” 할 수 있도록 하고 있다. 또한, “공공정보 개방·공개 시에는 특정 개인을 알아볼 수 있는 요소를 삭제하거나 비식별화 처리 후 개방·공개 가능” 하도록 하고 있다. 그러나 이는 개인정보의 목적 외 이용 및 제공에 해당해 개인정보 보호법 위반이 될 수 있다.

이후 2014년 12월 행정자치부와 한국정보화진흥원이 <개인정보 비식별화에 대한 적정성 자율평가 안내서>를 발표했다. 상기 2013년의 지침이 공공정보의 활용을 위한 것이라면, 이 안내서는 공공 및 민간의 개인정보처리자 모두를 대상으로 하고 있다. 여기서도 비식별화, 익명화, 재식별화를 구분했으며 익명화는 “비식별화 조치의 궁극적인 상태로 개인에 대한 재식별이 더이상 불가능한 상태” 로 규정했다.

2014년 방송통신위원회에서 추진한 <빅데이터 개인정보보호 가이드라인>은 공개된 개인정보, 이용내역 정보, 그리고 이 정보들의 분석을 통해 새로 생성된 정보 등의 처리 원칙을 규정하고자 한 것이었다. 이 가이드라인은 비식별화를 “데이터값 삭제, 가명처리, 총계처리, 범주화, 데이터 마스킹 등을 통해 개인정보의 일부 또는 전부를 삭제하거나 대체함으로써 다른 정보와 쉽게 결합해도 특정 개인을 식별할 수 없도록 하는 조치” 로 규정했다. 그런데 비식별화 조치를 한 경우에는 개인정보 법제의 적용을 배제하도록 하고 있어서, 시민사회단체에서는 이 가이드라인이 빅데이터 산업 활성화를 위해 개인정보 법제를 훼손하는 행정행위라며 반발했다[105].

105) 경실련, 진보네트워크센터, 함께하는시민행동, 2013.12.30., “방통위의 빅데이터 개인정보보호 가이드라인(안)에 대한 시민단체 입장”, <http://act.jinbo.net/wp/7753/>.

나. 개인정보 비식별 조치 가이드라인

2016년 6월, 박근혜 정부에서 정부 부처 합동(국무조정실, 행정자치부, 방송통신위원회, 금융위원회, 미래창조과학부, 보건복지부)으로 발표한 <개인정보 비식별 조치 가이드라인>은 기존에 서로 다른 기관에서 다뤘던 가이드라인을 통합한 것으로 볼 수 있다.

이 가이드라인은 빅데이터 분석에 활용하기 위해 서로 다른 정보집합물(데이터셋)을 결합하는 공공기관 및 민간 기업의 업무를 지원하기 위해 개인정보 비식별 조치 전문기관을 설립하도록 했다. 이 가이드라인은 비식별 조치에 대해 "정보집합물에서 개인을 식별할 수 있는 요소를 전부 또는 일부 삭제하거나 대체하는 등의 방법을 활용, 개인을 알아볼 수 없도록 하는 조치"로 규정하고 있으며, 이 가이드라인에 따라 정보주체를 알아볼 수 없도록 비식별 조치를 적정하게 한 비식별 정보는 "개인정보가 아닌 것으로 추정"되며, 따라서 빅데이터 분석 등에 이용하거나 제3자에게 제공할 수 있다고 한다. 동시에 불특정 다수에게 공개하는 것은 식별 위험이 크므로 원칙적으로 금지하고, 비식별 조치된 정보가 유출되는 경우 다른 정보와 결합해 식별될 우려가 있으므로 필수적인 보호조치를 이행하도록 하고 있다. 즉, 비식별 정보가 여전히 재식별의 가능성이 있음을 인지하고 있음에도 불구하고, 개인정보가 아닌 것으로 추정해 개인정보 보호법의 적용을 배제하고 있는 것이다.

가이드라인 발표 후인 2016년 8월, 각 부처에 의해 개인정보 비식별 조치 전문기관이 지정됐으며, 9월에는 전반적인 운영 지원을 위해 한국인터넷진흥원(KISA)에 '개인정보 비식별 조치 지원센터'가 설치됐다. 그리고 동 가이드라인에 의해 2016년 8월부터 2017년 9월까지 26차례에 거쳐 총 3억4천7백5십2만2천5건의 기업 데이터가 결합된 것으로 나타났다[106].

그러나 이 가이드라인은 개인정보 보호법의 위임 범위를 벗어났다는 비판을 받았다. 비식별 조치의 개념이 개인정보 보호법에 근거가 없을 뿐만 아니라, 비식별 처리된 정보로 인한 개인정보 침해가 발생할 경우 법적 책임을 누가 질 것인지 모호했기 때문이다. 특히 결합에 사용되는 정보집합물의 경우 임시대체키를 사용하여 특정 개인을 식별할 수 있도록 하기 때문에 익명정보로 보기에는 무리가 있다. 따라서 전문기관을 통한 정보집

106) 이은우 외(2017), 데이터 연계/결합 지원제도 도입방안 연구, 개인정보보호위원회 연구 용역, p44.

합물의 결합은 정보주체의 동의없는 제3자 제공으로서 개인정보 보호법 위반 소지가 있었다.

이에 시민사회단체들은 2017년 11월 비식별 전문기관과 20개 기업을 개인정보 보호법 등 위반으로 검찰에 고발하였다.[107] 이후 가이드라인이 공식적으로 폐지되진 않았지만 사실상 사문화됐다.

2. 가명정보 개념의 도입

가. 규제·제도혁신 해커톤에서의 논의

문재인 정부 역시 빅데이터 환경에서 개인정보 활용을 활성화하려는 움직임을 보이며 대통령 산하에 4차산업혁명위원회를 두었다. 4차산업혁명위원회는 '규제·제도혁신 해커톤'이라는 이름으로 4차 산업혁명 관련 주요 이슈에 대해 정부, 산업계, 시민사회, 학계 등 관련 이해관계자들이 모여 끝장 토론 방식으로 합의를 모으는 행사를 개최했다. '개인정보의 보호와 활용의 조화'를 의제로 두 차례에 걸쳐 해커톤이 열렸다.

<2차 해커톤 합의 내용>

① 개인정보 관련 법적 개념체계 정비

개인정보와 관련된 법적 개념체계는 개인정보, 가명정보, 익명정보로 구분하여 정비하기로 하였다. 그리고 익명정보는 개인정보 보호법의 적용대상이 아니라고 합의하여 개인정보와 구분하였다.

② 익명정보 개념은 법에 명시하지 않음

'익명정보' 개념을 명확히 하기 위하여 '익명정보' 정의를 법에 명시하는 대신 EU GDPR 전문(26)을 참조하여 '개인정보'의 개념을 보완하기로 논의하였다.

③ '가명정보'에 대한 법적 근거 마련

'가명정보'의 정의 및 활용에 관한 법적 근거를 마련하기로 하였다.

④ 개인정보의 보호와 활용에 대한 지속적 논의 진행

개인정보 보호와 활용에 관한 주요 이슈들에 대해서 추가적인 논의를 진행하기로 하였다.

107) 검찰은 2019년 3월 25일, 이 고발에 관하여 혐의없음(증거불충분) 불기소처분 결정을 통지했다. 그러나 시민사회단체들은 이는 동의 없는 개인정보 결합 및 제3자 제공에 면죄부를 준 것이라며 검찰을 규탄하였다. 건강사회를위한약사회 외, 2019.4.1., "정보주체의 동의 없는 개인정보 결합 및 제3자 제공에 면죄부 준 검찰을 규탄한다", <https://act.jinbo.net/wp/40717/> 참조.

2차 해커톤에서는 비식별화라는 용어보다는 ‘개인정보, 가명정보, 익명정보’로 개인정보와 관련된 법적 개념체계를 정비하기로 합의했다[108].

큰 틀에서의 합의는 이루어졌으나, 여러 의제에 대한 상세한 논의가 이루어지지는 못했기 때문에 3차 해커톤에서 개인정보 이슈가 다시 다루어졌다[109]. 가명정보의 활용과 보호, 익명처리의 절차·기준·평가, 데이터 결합, 개인정보 보호 체계 등의 이슈가 토론됐는데 이 모든 의제에 대한 합의가 도출된 것은 아니었다. 특히 가명정보의 활용 목적과 범위가 쟁점이 됐다.

<3차 해커톤 합의 내용>

가. 가명정보의 활용 목적과 범위

가명정보는 ① 공익을 위한 기록 보존의 목적, ② [학술 연구/학술 및 연구]* 목적 ③통계 목적을 위하여 당초 수집 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다고 합의하였다.

* 학술 연구/ 학술 및 연구 목적에서 연구의 범위에 관하여 이견이 있어 참석자 일부는 ‘학술 연구’라는 표현을, 다른 일부는 ‘학술 및 연구’라는 표현을 지지하였다.

그리고 이를 위해서는 가명처리를 포함한 기술적, 관리적 조치 등 안전조치가 취해져야 한다는 점에 동의하였다.

나. 최초 수집목적과 양립되는 추가적인 개인정보 처리

정부는 유럽연합 일반개인정보 보호법(EU GDPR)등 해외 입법례를 참조하여, 가명처리 여부 등 여러 사정을 고려해 개인정보를 당초 수집한 목적과 상충되지 아니하는 목적으로 활용할 수 있도록 하는 제도를 마련한다는 점에 합의하였다.

시민사회 참석자들은 개인정보인 가명정보를 당초 수집 목적 외 용도로 이용하거나 제3자에게 제공하는 것은 정보주체의 권리를 일정하게 제약하는 것이기 때문에 이를 허용하려면 사회 전체에 혜택을 주는 공익적 가치가 있는 ‘학술 연구 및 통계 작성’으로 활용 범위를 제한해야 한다는 입장이었다. 반면 산업계는 빅데이터 산업 발전을 위해 산업적 연구 및 시장 조사 등으로 폭넓게 허용해야 한다고 주장했다.

익명처리와 관련해서는 <개인정보 비식별조치 가이드라인>과 같이 특정 가이드라인에 따르면 무조건 익명정보라고 간주하는 것이 아니라, 개인정보처리자가 책임을 지는 것으

108) 이에 대해서는 4차산업혁명위원회 관련 페이지 https://www.4th-ir.go.kr/topic/6/detail/11 참조.

109) 이에 대해서는 4차산업혁명위원회 관련 페이지 <https://www.4th-ir.go.kr/topic/7/detail/13> 참조.

로 하였다. 정부가 익명처리의 적정성을 평가하기 위한 절차와 기준을 마련할 수는 있지만, 이러한 절차와 기준은 기술적 중립성에 입각한 것이어야 하며, 강제적인 것이거나 최종적인 것으로 해석되어서는 안 된다고 합의했다.

데이터 결합과 관련해서도 합의에 이르지 못했다. 시민사회는 데이터 연계는 개인정보 침해 위험성이 높고, 해외에서는 민간 기업의 데이터를 결합하거나 특히 이를 공공기관이 지원하는 사례를 찾기 힘들기 때문에 국내에서도 섣불리 허용해서는 안 된다는 입장이었다. 반면, 산업계는 민간 기업의 데이터 연계도 허용하되 절차적인 통제 방안을 마련하자고 주장했다.

개인정보 보호 체계와 관련해서는 정보통신망법, 신용정보법, 위치정보법은 각 부문에서 고유하게 규정할 필요가 있는 사항을 제외하고는 개인정보와 관련한 중복·유사 조항에 대해 통일이 필요하다는 점에는 합의했으나 구체적인 방안까지 논의하지는 못했다. 그러나 해커톤은 사회적 논의를 위한 공간일 뿐 정책을 결정하는 곳은 아니기 때문에, 궁극적으로는 각 정부 부처에서 해커톤에서의 합의를 반영하여 정책 방안을 수립하고, 국회에서 관련 법제를 개정하는 것이 필요했다.

나. 국회 4차 산업혁명 특별위원회

2017년 11월 구성된 '국회 4차산업혁명 특별위원회'는 4차 산업혁명에 대응하기 위한 정책 및 입법 권고를 위해서라는 명목으로 만들어졌다. 2018년 5월 활동을 종료한 특위는 <국회 4차 산업혁명 특별위원회 활동결과보고서>를 발표했다. 이 보고서에는 정책 및 입법권고안이 담겨 있는데, 특히 개인정보의 보호와 활용 관련한 특별권고안이 포함되어 있다. 이 권고안은 개인정보 보호와 활용에 관한 전향적인 규제 개혁이 필요하고 신뢰에 바탕을 둔 '개인정보의 안전한 활용'의 실행이 시급하다며 5건의 정책권고와 4건의 입법 권고를 채택했다.

3. 데이터 3법의 제정

20대 국회에 개인정보 보호와 관련한 법안이 여러 개 발의됐다. 소병훈, 송희경, 변재일, 진선미, 인재근, 이재정 의원 등이 개인정보 보호법 개정안을 발의했다. 개인정보 보

호법 개정 흐름과 동시에 신용정보법, 정보통신망법 개정도 추진됐다. 해커톤에서의 논의 이후 정부도 개인정보 보호 법제의 개정을 추진했는데, 그 대략적인 방향은 2018년 8월 31일 있었던, 문재인 대통령의 '데이터 경제 활성화 규제혁신 현장방문 행사'에서 제시되었다[110]. 이날 행사에서 문재인 대통령은 대한민국이 데이터를 가장 잘 다루는 나라가 되어야 한다고 강조하였고, 정부 부처는 공동으로 데이터 활용 관련 규제혁신 방안을 발표하였다. 정보주체의 동의없이 활용할 수 있는 가명정보 개념을 도입하고, 통계작성(시장조사 등 상업적 목적 포함), 연구(산업적 연구 포함) 등 가명정보를 활용할 수 있는 범위를 구체적으로 입법화하겠다는 것이다[111]. 이와 함께 구체적인 내용은 없었지만, 개인정보 보호위원회의 위상 강화로 개인정보 보호를 강화하겠다고 표명하였다.

정부가 '개인정보의 활용'에 초점을 두었다면 시민사회단체는 개인정보 보호 법제의 정비와 감독기관의 통합을 촉구했다[112]. 정부의 데이터 정책은 2018년 11월 3개 법안의 개정안으로 구체화 되었다. 2018년 11월 15일 인재근 의원이 대표발의한 개인정보 보호법 개정안(의안번호 16621), 노웅래 의원이 대표발의한 정보통신망법 개정안(의안번호 16622), 김병욱 의원이 대표발의한 신용정보법 개정안(의안번호 16636)이 그것이다. 정부는 이 세 가지 법을 하나로 묶어 '데이터 3법'이라고 칭했다. 반면, 시민사회단체들은 이를 '개인정보 도둑법'이라 비판하였다[113].

인재근 의원안에는 통계 작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있도록 하는 내용이 담겨 있었다. 정보통신망법의 개인정보 관련 조항은 개인정보 보호법으로 통합되었다. 개인정보 보호위원회는 국무총리 소속 중앙행정기관으로 격상되었으며, 행정안전부 및 방송통신위원회의 감독권한은 개인정보 보호위원회로 일원화되었다. 그러나 금융위원회의 개인신용정보에 대한 감독권한은 존속되었고, 개인정보 보호법과 신용정보법의 중복과 혼란은 해소되지 못했다.

---

110) 청와대, 2018.8.31., "데이터경제 활성화 규제혁신 현장방문 인사말", <https://www1.president.go.kr/articles/4122>.

111) 과학기술정보통신부 외, 2018.8.30., "데이터를 가장 안전하게 잘 쓰는 나라를 만들겠습니다. - 데이터 경제 활성화 규제혁신 현장방문 행사 실시 -", <https://www.korea.kr/news/pressReleaseView.do?newsId=156291739>.

112) 경제정의실천시민연합 외, 2018.5.17., "빅데이터 활성화 위해 개인정보 보호체계와 감독기구 일원화 시급하다!", <https://act.jinbo.net/wp/38647/>.

113) 건강과대안 외, 2019.12.9., "개인정보 도둑법 강행하는 정부 규탄한다", <http://www.peoplepower21.org/PublicLaw/1673757>.

데이터 3법은 시민사회의 반대와 국회 논의 과정에서의 논란에도 불구하고, 결국 2020년 1월 9일 국회를 통과하였다. 그러나 법안 통과 과정에서 국회 과학기술정보방송통신위원회 및 법제사법위원회에서 문제제기가 이루어지기도 했다. 특히 과학기술정보방송통신위원회는 2019년 12월 4일, 정보통신망법 개정안을 의결하면서, 개인정보 보호법 개정안에 대한 부대의견을 제안하였다. 하지만 이 부대의견은 법제사법위원회 논의 과정에서 전혀 개정안에 반영되지 못했다. 다만, 의원들이 생각하는 개인정보 보호법의 문제점과 개선 제안을 담고 있다는 점에서, 향후 개인정보 보호법 개정 과정에서 참고할 필요가 있다[114].

1. 법 적용대상자인 개인정보처리자와 정보통신서비스 제공자의 용어 개념에 대한 혼선이 야기될 가능성이 있으므로 향후 정합성 제고 차원에서 재검토 및 이에 대한 개선이 필요함
2. 개정안 제28조의2 제1항에 "정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 없는 경우에 한하여" 라는 조건을 추가하여 가명정보 처리 시에 정보주체의 권리가 보호될 수 있도록 하는 것이 바람직함
3. 가명정보의 목적 외 이용 또는 제3자의 제공 처리 시에 이를 공표하도록 하는 조항, 개인정보 프로파일링(profiling)의 정의 신설 및 개인정보 프로파일링으로 인한 정보주체 권리침해 방지에 대한 조항을 추가로 반영하는 것이 바람직함
4. 제28조의4 제1항 위반의 경우, 동일한 위반행위에 대하여 형사처벌(징역형 ·벌금)과 행정처분(과태료)을 동시에 부과하고 있으므로 법리적 차원에서 개선이 필요함
5. 제28조의4 제2항을 위반할 경우 형사처벌 대신 과태료 부과만 가능하게 되는데 기록을 작성·보관하지 않은 가명정보 처리자에게 과태료를 부과하는 것은 '정보제공자 본인의 동의 없이' 처리할 수 있는 가명처리의 특성상 매우 낮은 수준의 처분이므로 이에 대한 개선이 필요함
6. 제28조의5 제1항의 경우 "누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리하여서는 아니된다" 고 규정하여 특정 개인을 알아보기 위한 목적만 없다면 특정 개인을 알아볼 수 있는 정보를 생성해도 과태료 부과에 그치므로 이에 대한 개선이 필요함

114) ZDNET Korea, 2019.12.4., "정보통신망법도 상임위 통과…'데이터 3법' 모두 법사위로", <https://zdnet.co.kr/view/?no=20191204160257>.

제2절 데이터 3법의 주요 쟁점 및 문제점

1. 개인정보 보호 체계의 개선과 한계

가. 과거 개인정보 보호 체계의 문제점

그동안 한국의 개인정보 보호 체계의 문제점으로 연구자들과 시민사회에서 일관되게 지적해온 문제는 다원적인 개인정보 보호 법제로 인한 혼란과 독립적인 감독기관의 부재였다. ‘데이터 3법’은 이와 같은 개인정보 보호 체계의 문제를 일부 개선하기는 했으나 말끔하게 해결하지는 못했다.

2011년 제정된 개인정보 보호법은 공공부문과 민간부문의 모든 개인정보처리자에게 적용되는 법으로 개인정보의 수집, 이용, 제공 등 개인정보 처리 단계에 따른 보호의 기준을 구체화하였다. 특히 정보주체의 개인정보 침해가 우려되는 경우 공공기관에 대해 개인정보 영향평가를 위한 적극적인 노력을 요구하는 등 개인정보의 효율적인 보호를 위한 수단을 포함하고 있다[115]. 그러나 일반법인 개인정보 보호법 제정과 함께 기존에 개별 영역을 규율했던 법률, 즉 정보통신망법, 신용정보법 등 타 법률의 개인정보 관련 조항을 함께 정비해야 했지만 그렇게 하지 못했고, 여전히 각 개별법들이 유지되었다. 또한, 개인정보 보호법에 따라 대통령산하 개인정보 보호위원회가 설립되기는 했지만 ‘개인정보 보호에 관한 법령의 해석, 운용에 관한 사항의 심의, 의결’ 등 일부 권한만을 부여했을 뿐, 여전히 개인정보 보호법의 관할 부처이자 감독기관으로서의 집행권한은 행정안전부에 있었다.

이와 같은 상황에 대해 다음과 같은 여러 문제가 지적되었다. 첫째 법제 간에 중복·유사 규정이 존재해 수범자의 혼란을 초래하거나 모든 법률을 준수해야 하는 부담을 야기하게 된다는 점이다. 동일한 행위에 대해 법률에 따라 벌칙이 상이한 경우가 발생하며, 상이한 제재조치는 법의 집행에 있어 형평성을 저해하는 문제로 이어질 수 있다. 예를 들어, 정보주체의 동의 없이 개인정보를 수집한 경우, 개인정보 보호법은 제75조에서 5천만 원 이하 과태료를 부과하고 있는 반면, 정보통신망법 제71조는 5년 이하의 징역 또

115) 이인호 외(2017), 한국의 개인정보보호 수행체계 발전방안 연구, 개인정보 보호위원회 연구용역보고서

는 5천만 원 이하의 벌금에 처하도록 하고 있다. 이 경우 수범자는 기준으로 삼아야 할 법률을 파악하기 힘들게 되며, 위법사항이 발생하는 경우에도 어떤 법을 기준으로 벌칙이 정해지느냐에 따라 그 수준이 상이한 경우가 발생한다.

둘째, 조항의 해석 및 법률 적용의 우선순위에 있어 혼란을 초래한다. 개인정보 보호법 제6조는 '다른 법률과의 관계'를 다른 법에서 정한 바가 없다면 개인정보 보호법이 우선하도록 규정하고 있는데, 만일 정보통신망법 등 다른 법률을 특별법으로서 우선 적용한다면 일반법으로서 개인정보 보호법이 유명무실해지는 결과를 초래할 수 있다.

셋째, 각 법률의 소관 부처가 달라 규제기관 간 규제영역 확보를 위한 경쟁을 하거나, 국회의 개별 상임위원회에서 전체적인 개인정보 보호 체계에 대한 고려 없이 법 개정이 이루어짐에 따라 법률 간의 차이가 심화하고 있었다. 실제로 2011년 개인정보 보호법 제정 이후에도 행정안전부, 방송통신위원회, 금융위원회는 30여 차례가 넘도록 경쟁적으로 법률 및 시행령 개정을 추진한 바 있다[116].

넷째, 개인정보 보호법을 제외한 다른 법률들은 대부분 개인정보 보호 규정과 동시에 각 산업의 진흥을 위한 내용을 함께 고려하고 있어 각 부문마다 개인정보 보호 관련 정책의 불일치가 발생할 수 있다[117]. 즉, 4차 산업혁명과 관련한 신기술을 발전시키기 위해 빅데이터 활용 및 개인정보 활용을 추진하는 한편 개인정보 보호를 위한 방안을 강구해야 하는 상황이 되는데, 이 경우 개인정보 보호에 방점을 두기보다는 해당 산업의 발전에 더 집중해 정책을 추진하는 경우가 나타날 수 있다. 예를 들어 개인정보의 결합·분석을 통해 통합적인 금융 데이터베이스를 구축하고자 할 경우, 이 과정에서 나타날 수 있는 여러 문제에 관해 고민하고 규정하는 대신 개인신용정보 활용을 위한 개인정보 비식별 조치를 지원하는 데만 역점을 둘 수 있다.

혼란스러운 개인정보 보호 법제와 함께, 분산된 개인정보 감독기관의 문제도 오래동안 문제로 지적되었다. 개인정보 보호법에 따라 대통령 소속의 개인정보 보호위원회와 행정안전부가 개인정보 감독기관의 역할을 수행하고 있는 동시에, 민간 정보통신분야의 개인정보 보호 업무는 방송통신위원회, 개인신용정보에 대한 감독은 금융위원회가 담당하고 있는 등 분산되어 있었다. 이러한 분산된 체제는 개인정보처리자의 법 준수 어려움, 대

116) 이은우 외(2018), 앞의 글, p101.
117) 김일환(2017), 현행 개인정보보호법체계상 감독기구 법제정비방안에 관한 연구, 미국헌법연구 제28권 2호, pp219-273.

규모의 개인정보 침해사고 발생 시 컨트롤타워 부재, 개인정보 감독기관의 독립성과 자율성 문제 등 여러 문제를 야기했다[118].

개인정보 감독기관과 관련하여 무엇보다 큰 문제는 독립성이 부재하다는 것이었다. 개인정보 감독기관과 관련된 국제 규범은 감독기관의 독립성을 핵심적인 요건으로 규정하고 있다. GDPR 역시 유럽사법재판소 판결 등을 통해 확립된 감독기관에 관한 규범을 반영하고 있는데, ▲ 감독기관의 완전한 독립성, ▲ 직무권한의 독립성, ▲ 양립불가 업무의 겸직금지, ▲ 직무 수행 및 권한 행사에 필요한 인적, 기술적 및 재정적 지원 보장, ▲ 직원 인사의 자율성, ▲ 예산의 독자성 등을 독립성 요건으로 규정했다[119]. 그러나, 행정안전부의 경우 스스로가 국민의 방대한 정보를 보유하고 있는 개인정보처리자이자 국무총리의 지휘를 받고있는 중앙행정기관이기 때문에 독립성을 보장하기 어렵다. 방송통신위원회와 금융위원회는 형식상 독립적인 합의제 행정기관이긴 하지만, 산업 육성의 역할을 동시에 담당하고 있어 산업 육성을 위해 개인정보 규제를 완화하려 한다는 비판을 받아왔다. 개인정보 보호위원회는 인사·예산권 등을 보유하고 있지 않아 독립성이 없고, 업무 역시 개선 권고, 의견 조정 등에 집중돼 있어 권한이 매우 약했다. 실제 개인정보 관리 수준을 파악하기 위한 조사 권한, 위반행위 조사를 위한 자료제출 요구권 및 감사권, 과태료 부과 등 주된 집행 권한은 행정안전부가 보유하고 있었다.

나. 데이터 3법으로 인한 보호 체계 개선과 한계

이와 같은 문제점을 해결하기 위해 신기술에 대응하기 위한 법제 개선에 앞서서 분산된 개인정보 보호 법제 및 감독체제를 체계적이고 통일적으로 정비할 필요성이 오랫동안 제기되어 왔다. 데이터 3법은 이 두 가지 문제를 해결하려는 취지로 발의되었다. 2020년 1월 9일 통과한 개정 개인정보 보호법[120]은 그 입법취지(개정이유)를 다음과 같이 설명하고 있다. “정보주체의 동의 없이 과학적 연구, 통계작성, 공익적 기록보존 등의 목적으로 가명정보를 이용할 수 있는 근거를 마련하되, 개인정보처리자의 책임성 강화 등 개인정보를 안전하게 보호하기 위한 제도적 장치를 마련하는 한편, 개인정보의 오용·남용

118) 권건보 외(2017), 지능정보사회 대응을 위한 개인정보보호 법제 정비방안, 개인정보보호위원회 연구용역.
119) 이은우 외(2018), 앞의 글, p25.
120) 의안번호 2024495. 개인정보 보호법 일부개정법률안(대안)(행정안전위원장).

및 유출 등을 감독할 감독기구는 개인정보 보호위원회로, 관련 법률의 유사·중복 규정은 이 법으로 일원화함으로써 개인정보의 보호와 관련 산업의 발전이 조화될 수 있도록 개인정보 보호 관련 법령을 체계적으로 정비하려는 것임."

2011년에 개인정보 보호법이 제정될 때부터 2020년 개정될 때까지 거의 10년 동안 개인정보 보호 법제와 감독기관의 통합이 지연된 것은 기존에 권한을 갖고 있던 정부 부처의 조직이기주의 때문으로 볼 수 있다. 2018년 초 해커톤이 개최될 당시만 해도 정부 부처 참여자들은 감독체계 개선방안을 안건으로 올리는 것조차 반대하였다. 그런데 2018년 말에 발의된 데이터 3법에서 부분적으로나마 법제 및 감독기관의 통합이 이루어진 것은 무엇 때문일까. 표면적인 측면에서 본다면, 개정이유에 표현되어 있는 바와 같이 가명정보를 이용할 수 있는 근거를 마련하는 반대 급부로서 개인정보의 오남용에 대한 감독을 강화하겠다는 취지로 볼 수 있다. 그러나 기존의 정부 부처 역시 빅데이터 등 산업활성화와 개인정보의 보호를 함께 거론해왔다는 점에서 이와 같은 표면적인 이유만으로는 설명하기 힘들다. 정부에서 부처간의 이해관계를 일정하게 조정할 수 있었던 이유는 아마도 유럽연합의 GDPR에 따른 개인정보 적정성 결정을 체결하기 위해 독립적인 감독기관이 필요하다는 압력이 존재했기 때문일 것으로 추정할 수 있다. 물론 독립적인 감독기관의 설립은 학계 및 시민사회에서 오랫동안 요구해온 것이기 때문에 이를 추진할 명분도 있었다.

유럽연합 개인정보 적정성 결정 체결을 위해 처음부터 개인정보 보호위원회 강화를 추진했던 것은 아니다. 한국 정부는 이미 2015년 8월에 '**EU 적정성 평가 민·관 합동추진단**'을 구성하고 개인정보 보호법을 중심으로 '**전체 적정성 결정**'을 추진하였다[121]. 그러나 2016년 10월, 유럽집행위원회로부터 부적격 통지를 받았는데, 한국의 개인정보 감독기관이 독립성이 없고 권한이 미비하다는 이유에서였다. 이에 정부는 2017년 3월 방송통신위원회 주관으로 정보통신망법을 중심으로 '**부분 적정성 결정**'을 추진하기로 방향을 전환하였다[122]. 이에 2017년 11월 13일, 개인정보 보호위원회는 부분 적정성 결정 추진을 중단하고, "개인정보 보호위원회의 직권조사권, 운영 독립성 등 기본권한 확충 등에 대한 정부 의사결정 절차를 거쳐 전체적정성 결정으로 재전환" 할 것을 행정

121) 이은우 외(2018), 앞의 글, p60.
122) 개인정보보호위원회 결정(2017), EU 부분적정성 평가 전환 추진 개선에 관한 건, 제2017-25-198호.

안전부와 방송통신위원회에 권고하였다. 개인정보 보호위원회는 “부분적정성 결정은 그 효과가 제한적이고 개인정보 보호기관의 완전한 독립성 확보, 직권조사권 등 실질적 보호기능 수행을 보장하는 국제사회의 흐름과 개인정보 보호위원회를 컨트롤타워로 하여 개인정보 보호 체계 효율화를 목표로 하는 국정과제에 배치될 뿐만 아니라 개인정보 보호법과의 적용 혼란 등 부작용이 예상” 된다고 비판하였다. 결국 청와대의 중재로 우선 방송통신위원회 중심의 부분 적정성 평가를 추진하고, 동시에 행정안전부, 방송통신위원회, 개인정보 보호위원회 등이 TF를 구성하여 전체 적정성 추진을 위한 준비를 병행하는 것으로 부처 간 합의를 하였다[123]. 그러나 방송통신위원회가 추진해 온 ’부분 적정성 평가’ 역시 유럽연합으로부터 거부당한 것으로 보인다[124]. 그래서 유럽연합과 적정성 결정을 체결하기 위해서는 개인정보 보호위원회의 독립성과 권한을 강화하는 방안밖에 남지 않은 것이다.

2020년 1월 데이터 3법 통과로 개인정보 보호 법제의 통합과 독립적인 감독기관의 설립이 일부 이루어졌다. 그러나 보호 법제와 감독기관의 일원화라는 관점에서는 미흡한 점이 많다. 첫째, 정보통신망법은 개인정보 보호법으로 통합이 되었지만, 신용정보법의 개인정보 관련 조항은 여전히 남아있으며 금융위원회 역시 개인신용정보에 대한 감독권한을 유지하고 있다. 금융위원회는 금융기관에 대한 감독과 개인신용정보에 대한 감독이 동시에 이루어지는 것이 효율적이라고 주장하지만 이는 설득력이 없다. 이런 논리라면 정보통신, 의료, 교육 등 다른 분야에서도 기존의 정부 부처가 개인정보 감독기관의 역할을 해야 할 것이다. 또한 개인정보 보호위원회가 단일한 개인정보 감독기관으로서 컨트롤타워 역할을 한다고 해서 각 정부 부처가 소관 영역의 개인정보 감독의 역할을 하지 못하는 것도 아니다. 개인정보 보호법 제61조 제3항은 관계 중앙행정기관의 장이 개인정보 보호를 위하여 필요하다고 인정하면 소관 법률에 따라 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있도록 하고 있다. 제4항에서는 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관에 대하여 개인정보 보호에 관한 의견을 제시하거나 지도·점검을 할 수 있도록 하고

123) 전자신문, 2017.12.5., “개인정보보호위원회, 정부 EU GDPR 적정성평가 전략 이견 제기…위원회 독립성 문제도 불거져”, <http://www.press9.kr/news/articleView.html?idxno=33043>.

124) 미디어 오늘, 2018.11.2., “방통위 밀어붙인 개인정보 평가, EU에서 ‘퇴짜’”, <http://www.mediatoday.co.kr/news/articleView.html?idxno=145317>.

있다.

둘째, 데이터 3법은 개정이유로 “관련 법률의 유사·중복 규정의 개인정보 보호법으로의 일원화”를 천명했지만, 오히려 개인정보 보호법과 신용정보법 개정안 자체가 유사·중복 규정으로 인한 혼란을 심화시켰다. 예를 들어, 개인정보의 정의에서부터 두 법의 규정이 유사하지만 차이가 있으며, 개인정보 보호법에는 익명처리의 개념이 없지만 신용정보법에서는 두고 있다. 개인정보 보호법에서는 ‘과학적 연구’라는 개념을 사용하고 정의 규정을 두고 있지만, 신용정보법은 정의 규정 없이 ‘연구’라는 개념을 사용하고 있다. 아래 표는 개인정보 보호법과 신용정보법이 차이를 보이는 주요 조항의 일부를 정리한 것이다.

<표3-1> 개인정보 보호법과 신용정보법의 주요 조항 비교

개인정보 보호법	신용정보법
제2조(정의) 1. “개인정보“란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다. 가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보 나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다. 다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 “가명정보“라 한다)	제2조(정의) 2. “개인신용정보“란 기업 및 법인에 관한 정보를 제외한 살아 있는 개인에 관한 신용정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다. 가. 해당 정보의 성명, 주민등록번호 및 영상 등을 통하여 특정 개인을 알아볼 수 있는 정보 나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보
제58조의2(적용제외) 이 법은 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보에는 적용하지 아니한다.	제2조(정의) 17. “익명처리“란 더 이상 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리하는 것을 말한다.
제2조(정의) 1의2. “가명처리“란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을	제2조(정의) 15. “가명처리“란 추가정보를 사용하지 아니하고는 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리(그 처리 결과가 다음 각

말한다.	목의 어느 하나에 해당하는 경우로서 제40조의2제1항 및 제2항에 따라 그 추가정보를 분리하여 보관하는 등 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리한 경우를 포함한다)하는 것을 말한다. 가. 어떤 신용정보주체와 다른 신용정보주체가 구별되는 경우 나. 하나의 정보집합물(정보를 체계적으로 관리하거나 처리할 목적으로 일정한 규칙에 따라 구성되거나 배열된 둘 이상의 정보들을 말한다. 이하 같다)에서나 서로 다른 둘 이상의 정보집합물 간에서 어떤 신용정보주체에 관한 둘 이상의 정보가 연계되거나 연동되는 경우 다. 가목 및 나목과 유사한 경우로서 대통령령으로 정하는 경우
제2조(정의) 8. “과학적 연구“란 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 말한다.	없음
제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.	제32조(개인신용정보의 제공ㆍ활용에 대한 동의) ⑥ 신용정보회사등(제9호의3을 적용하는 경우에는 데이터전문기관을 포함한다)이 개인신용정보를 제공하는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 제1항부터 제5항까지를 적용하지 아니한다. 9의2. 통계작성, 연구, 공익적 기록보존 등을 위하여 가명정보를 제공하는 경우. 이 경우 통계작성에는 시장조사 등 상업적 목적의 통계작성을 포함하며, 연구에는 산업적 연구를 포함한다.
제28조의3(가명정보의 결합 제한) ① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.	제17조의2(정보집합물의 결합 등) ① 신용정보회사등(대통령령으로 정하는 자는 제외한다. 이하 이 조 및 제40조의2에서 같다)은 자기가 보유한 정보집합물을 제3자가 보유한 정보집합물과 결합하려는 경우에는 제26조의4에 따라 지정된 데이터전문기관을 통하여 결합하여야 한다.

셋째, 정보통신망법의 개인정보 관련 조항을 개인정보 보호법으로 흡수한 것은 바람직한 방향이지만, 개인정보 보호법의 관련 조항과 통합이 되었다기보다는 '제6장 정보통신서비스 제공자 등의 개인정보 처리 등 특례' 형식으로 포함되었기 때문에, 법은 통합되었으되 여전히 정보통신서비스 제공자인지 여부에 따라 별도의 취급을 받게 되는 상황은 해결되지 않았다. 재개정을 통해 유사 조항의 실질적인 통합이 필요하다.

넷째, 새로 출범한 개인정보 보호위원회의 독립성에 대해서도 우려가 제기되고 있다[125]. 개인정보 보호법은 개인정보 보호위원회가 개인정보에 관한 사무를 '독립적으로 수행'함을 명시하고 있고, 정부조직법 제2조에 따른 중앙행정기관으로 보되, 일부 업무에 대해서는「정부조직법」제18조를 적용하지 않는다는 규정을 두어 국무총리의 지휘, 감독권을 배제하고 있다. 그러나 「정부조직법」제18조를 적용하지 않는 사무는 정보주체의 권리침해에 대한 조사 및 이에 따른 처분에 관한 사항(제7조의8 3호), 개인정보의 처리와 관련한 고충처리·권리구제 및 개인정보에 관한 분쟁의 조정(제7조의8 4호), 개인정보 침해요인 평가에 관한 심의·의결에 한정하고 있다. 이렇게 되면 다른 업무, 예를 들어 개인정보 보호와 관련된 법령의 개선이나 정책을 추진하는데 있어서 국무총리의 지휘·감독을 받게 되며, 개인정보 보호위원회가 개인정보 감독기관으로서의 전문적인 관점이 아니라 정부의 정치적 지향에 영향을 받을 우려가 있다.

2. 개정 개인정보 보호법을 둘러싼 쟁점

가. 개인정보의 개념

2020년 1월 국회를 통과하여, 8월 5일 시행된 개정 개인정보 보호법은 '개인정보'를 다음과 같이 규정하고 있다.

> 제2조(정의) 1. "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
> 가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
> 나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼

125) 금융정의연대 외, 2020.2.17., "[개인정보보호법 개정 후속 과제]에 대한 시민사회 의견서", <http://act.jinbo.net/wp/42187/>.

수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보"라 한다)

개정 개인정보 보호법의 개인정보 정의 규정이 개정 이전과 달라진 점은 "이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다"라는 문구가 추가된 것과 '다' 목에서 가명정보 역시 개인정보임을 명확히 한 것이다.

그런데 이번 개정 이전부터 개인정보를 어떻게 해석할 것인지는 논란이 되어 왔다. 개인정보의 정의와 범위가 중요한 이유는 어떠한 정보가 개인정보가 아닌 것으로 간주될 경우 개인정보 보호법의 규율에서 벗어나 자유롭게 활용할 수 있기 때문이다. 2016년에 한국의 적정성 평가 준비를 위한 자체 평가보고서 작성에 참여했던 그린리프 교수는 적정성 평가 과정에서 문제가 될 수 있는 이슈 중의 하나로 개인정보의 개념 문제를 지적한 바 있다[126]. 그가 지적한 점은 개인정보의 정의에 '쉽게'라는 단어가 포함되어 있어서, 다른 정보와 '쉽게' 결합하여 알아볼 수 없는 한 개인정보가 아닌 것이 될 수 있기 때문에 개인정보가 유럽연합보다 더 좁게 정의될 수 있다는 것이다.

'쉽게'만을 따로 떼어내어 설명한 것은 아니지만, 한국 정부는 '쉽게 결합하여'의 의미에 대해 정보의 결합 대상이 될 '입수 가능성'이 있어야 하고 '결합 가능성'이 높아야 함을 의미한다고 해석하고 있다. 여기서 '입수 가능성'의 의미는 "두 종 이상의 정보를 결합하기 위해서는 결합에 필요한 정보에 합법적으로 접근·입수할 수 있어야" 함을 말하며, 해킹 등 불법적인 방법으로 취득한 정보는 배제한다. '결합 가능성'에 대해서는 "합법적인 방법으로 정보를 입수하여도 현재의 기술 수준에 비추어 결합이 사실상 불가능하거나, 결합하는데 비합리적인 수준의 비용이나 노력이 수반된다면 이는 결합이 용이하다고 볼 수 없"다고 한다. 그래서 "공유·공개될 가능성이 희박한 정보는 합법적 입수 가능성이 없다고 보아야 하며, 일반적으로 사업자가 구매하기 어려울 정도로 고가의 컴퓨터가 필요한 경우라면 '쉽게 결합'하기 어렵다고 보아야" 한다고 해

126) Graham Greenleaf(2018), Questioning 'adequacy' (Pt II) - South Korea.

석하고 있다[127]. 개정 개인정보 보호법의 정의에서 “이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려”해야 한다고 한 것은 이와 같은 기존 해석을 반영한 것이라고 볼 수 있다.

또한, 이 표현은 GDPR에 포함된 문구를 일부 반영한 것이기도 하다. GDPR 전문 26은 개인정보의 정의에 대해 아래와 같이 설명하고 있다.

GDPR recital 26

Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the mount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

가명화를 거친 개인정보는, 추가 정보를 사용하여 해당 자연인을 확인할 수 있는 경우 식별 가능한 자연인에 관한 정보로 간주되어야 한다. 자연인이 식별 가능한지 아닌지를 판단하기 위해서는, 자연인을 직간접적으로 식별하기 위해 컨트롤러나 다른 사람에 의해 사용될 합리적 가능성이 있는, 개인 특정(single out) 등 모든 수단을 고려해야 한다. 어떤 수단이 자연인을 식별하기 위해 사용될 합리적 가능성이 있는지 확인하기 위해서는, 처리 시점에 이용 가능한 기술과 기술 발전을 감안하여 식별에 필요한 비용과 시간 등 모든 객관적 요소를 고려해야 한다.

개인 식별에 필요한 시간, 비용, 기술 등을 합리적으로 고려하도록 한 이유는 어떤 정보가 그 자체로는 개인을 식별할 수 없지만 다른 정보와 결합하여 간접적인 방식으로 개인을 식별할 수 있을 때, 이처럼 간접적인 방식으로 개인이 식별 가능한(identifiable) 정보의 범위를 객관적으로 설정하기 쉽지 않기 때문이다. 특정 시점에서 개인 식별이 불가능할지라도 재식별 기술의 발전에 따라 미래에는 식별이 가능해질 수도 있다. 그래서

127) 행정안전부(2016), 개인정보 비식별 조치 가이드라인- 비식별 조치 기준 및 지원·관리체계 안내-, p55.

이처럼 특정 시점에 개인 식별을 위한 일정한 노력에도 불구하고 식별할 수 없는 경우에는 개인정보가 아닌 것으로 간주하는 것이 합리적이다. 이러한 기준은 기술의 발전에 따라 달라질 수 있다. 이와 관련하여 GDPR에서는 '처리 시점에 이용 가능한 기술과 기술 발전'을 모두 고려하도록 하고 있는데 한국의 개인정보 보호법은 간단히 '기술'만을 포함하고 있어 다소 좁게 규정한 것으로 볼 수 있는데, 이것이 실제 현실에서 어떠한 영향을 미칠지는 두고 볼 필요가 있다.

오히려 더 큰 차이점은 '누구의 관점'에서 알아볼 수 있는지, 즉 식별의 주체가 누구인지에 대한 것이다. 2016년 〈개인정보 비식별조치 가이드라인〉 안내서에서 정부는 '알아볼 수 있는'의 의미를 "해당 정보를 '처리하는 자'의 입장에서" 판단해야 한다고 해석하고 있다. 즉, 누군가는 특정 개인을 알아보기 위해 필요한 다른 정보를 가지고 있을지 몰라도 해당 정보를 '처리하는 자'의 입장에서 알아볼 수 없다면 개인정보가 아니라는 것이다. 2020년 통합 개인정보 보호위원회 출범 이후에 발간된 〈가명정보 처리 가이드라인〉[128]에서도 이러한 해석은 바뀌지 않았다. 이 가이드라인에서도 "개인을 '알아볼 수 있는지'는 해당 정보를 처리하는 자(정보의 제공 관계에 있어서는 제공받은 자를 포함)를 기준으로 판단하여야 함"이라고 언급하고 있다.

그런데 이는 GDPR에서의 해석과 차이가 있다. GDPR 전문 26에서는 "자연인을 직간접적으로 식별하기 위해 '컨트롤러나 다른 사람(by the controller or by another person)'에 의해 사용될 합리적 가능성"이 있는지를 판단한다. 한국 정부의 해석대로라면 유럽연합에서의 개인정보 정의보다 그 범위가 좁아질 수밖에 없다.

정부의 해석은 국내 법원의 판결과도 차이가 있다. 서울중앙지법은 스마트폰의 국제모바일기기식별코드(IMEI)나 가입자식별모듈(USIM) 일련번호가 개인정보에 해당하는지 여부에 대한 판결에서 '쉽게 결합하여'의 의미를 "쉽게 다른 정보를 구한다는 의미이기보다는 구하기 쉬운지 어려운지와는 상관없이 해당 정보와 다른 정보가 특별한 어려움 없이 쉽게 결합하여 특정 개인을 알아볼 수 있게 되는 것을 말한다"고 판시하였다[129]. 그리고 "IMEI나 USIM 일련번호와 관련된 개인에 관한 정보는 각 통신사별로 그 접근에 엄격한 통제를 가하고 있기는 하나, 제3자에 의하여 획득될 가능성이 없는 것으로 보이

128) 개인정보보호위원회(2020), 가명정보 처리 가이드라인, p17.
129) 서울중앙지법 2011.2. 23. 선고, 2010고단5343 판결.

지는 아니한 점”을 인정하여, IMEI와 USIM 일련번호 역시 개인정보라고 보았다. 이는 개인정보처리자의 관점에서 식별성을 판단해야 하며, 결합에 필요한 정보에 합법적으로 접근·입수할 수 있어야 한다는 정부의 해석과 차이가 있다.

유럽사법재판소도 유동 IP 주소가 개인정보인지 여부에 대한 판결에서 유사한 해석을 내렸다[130]. 이용자의 ISP만이 유동 IP 주소를 통해 이용자를 식별할 수 있지만, 유럽사법재판소는 온라인 미디어 서비스가 어떤 사람이 웹사이트에 접속할 때 동적 IP 주소를 기록할 경우 이를 개인정보로 보았다. 유럽사법재판소는 어떤 정보가 개인정보가 되기 위해서 “정보주체의 식별을 위한 모든 정보가 한 사람의 손에 있어야 하는 것은 아니다”라며, ISP가 “그 사람에 대한 추가 정보를 가지고 정보주체를 식별할 수 있는 법적인 수단을 가지고 있다면”, 이는 “정보주체를 식별하는데 합리적으로 사용될 가능성이 있는 수단”을 구성하며, 따라서 그러한 데이터는 개인정보라고 보았다[131].

개인정보 보호법의 개정안 논의 과정에서도 ‘식별의 주체’가 하나의 쟁점이었던 것으로 보인다. 인재근 의원이 대표 발의한 개인정보 보호법 개정안은 법의 적용 제외, 즉 개인정보가 아닌 익명정보에 대해 다룬 제58조의2(적용제외)에서 “이 법은 시간·비용·기술 등 개인정보처리자가 활용할 수 있는 모든 수단을 합리적으로 고려할 때 다른 정보를 사용하여도 더이상 개인을 알아볼 수 없는 정보에는 적용하지 아니한다”고 규정하였다. 그런데 법안 논의 과정에서 ‘개인정보처리자가 활용할 수 있는’이라는 문구가 삭제되고, “이 법은 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더이상 개인을 알아볼 수 없는 정보에는 적용하지 아니한다”는 표현으로 수정되었다. 이는 입법 과정에서 개인정보처리자를 식별의 주체로 보는 관점이 배척된 것으로 볼 수 있다. 이런 점에서 <가명정보 처리 가이드라인>에서 여전히 ‘개인정보처리자’ 관점에서 식별 가능한지 여부를 판단한다고 해석하는 것은 입법 의도와 배치되는 것으로 보인다.

개인정보의 개념을 넓게 해석하는데 대해 “규제 및 규범 준수로 인한 막대한 비용을 발생시키며, 정보의 흐름을 봉쇄하여 새로운 비즈니스 모델의 개발뿐만 아니라 기존의 거래마저 억제할 수 있으며, 최근 활용이 부쩍 증가하고 있는 빅데이터에 따른 혜택을

130) Patrick Breyer v. Bundesrepublik Deutschland(2016), C-582/14.
131) FRA(2018a) pp91-92.

크게 감소시킬 수 있다"는 반론이 제기된다[132]. 그러나 산업의 발전을 위해 기본권 침해 위험을 정당화할 수는 없다. 만일 어떤 정보를 보유하고 있는 개인정보처리자가 그 정보를 통해 특정 개인을 식별할 수 없다고 개인정보가 아닌 것으로 간주한다면, 개인정보 보호법의 규율을 받지 않을 것이므로 마음대로 공개해도 무방할 것이며, 그 결과 개인을 식별할 수 있는 다른 정보를 가지고 있는 자에 의해 정보주체의 권리가 침해당할 가능성을 배제할 수 없을 것이다.

물론 모든 개인정보에 대해서 개인정보 보호법이 동일하게 적용되는 것은 아니다. 가명처리와 같이 개인 식별 가능성을 낮추기 위한 처리를 할 경우 개인정보처리자의 책임이 좀 더 완화될 수 있을 것이다. 이처럼 개인정보가 야기할 수 있는 위험성에 비례하여 그에 대한 개인정보처리자의 책임을 완화하거나 특정한 활용을 가능하도록 열어줄 수는 있을 것이나, 개인정보성을 부정하는 것은 위험하다. 아예 개인정보 보호법의 적용 자체를 배제하게 되기 때문이다. 식별가능성이 있다면 개인정보임을 인정하되, 해당 정보의 식별 가능성이나 처리 목적 등에 따라 개인정보처리자의 책임을 달리하는 방식으로 접근하는 것이 타당할 것이다.

나. 가명처리와 가명정보의 의의

전술한 바와 같이 2018년 2월, 대통령직속 4차산업혁명위원회의 주관으로 개최된 2차 '규제·제도혁신 해커톤'에서 개인정보와 관련된 법적 개념체계를 정비하는 것에 합의하였다[133]. 이전 몇 년 동안 가이드라인 등에서 사용되어 왔던 '비식별'이라는 개념보다는 유럽연합 GDPR의 개념체계를 수용하여 개인정보, 가명정보, 익명정보라는 개념을 사용하기로 합의한 것이다. '비식별 조치'는 개인정보의 식별성을 제거하는 조치인데 비식별 조치의 수준에 따라 그 결과물이 여전히 개인정보일 수도 있고, 개인 식별이 불가능하도록 처리된 익명정보일 수도 있기 때문에 비식별 정보에 대한 법적 규율이 모호했기 때문이다. 2018년 11월 15일 발의된 개인정보 보호법 개정안(인재근 의원 대표발의)에도 가명처리, 가명정보의 개념이 포함되었다. 해커톤에서는 익명정보에 대해서는 그 개념을

132) 이대희(2015), 개인정보 개념의 해석 및 범위에 관한 연구, 고려법학 제79호, p173.
133) 4차산업혁명위원회, 2018.2.6., "4차산업혁명위, 제2차 규제.제도혁신 해커톤 개최 결과 - 개인정보 관련 법적 개념 체계 정비 합의, 전자서명법 개정을 통한 다양한 전자서명 활성화 방안 논의", <https://www.4th-ir.go.kr/pressRelease/detail/52>.

명시하는 것보다 GDPR 전문 26을 참조하여 개인정보의 개념을 보완하는 것으로 합의하였는데, 이는 익명정보가 결국 개인정보가 아닌 것을 의미하는 것이기 때문이다. 인재근 의원이 대표 발의한 개정안에서는 개인정보, 가명처리, 가명정보의 개념과 함께, 익명정보라는 개념을 사용하지는 않았지만 제58조의2(적용제외) 조항을 통해 개인을 식별할 수 없는 정보에는 개인정보 보호법이 적용되지 않음을 특별히 규정하였다. 그러나 제2조(정의) 1호에서 개인정보의 개념을 정의하고 있기 때문에 제58조의2(적용제외)가 없더라도 개인정보가 아닌 정보에는 개인정보 보호법이 적용되지는 않는다. 한편, 해커톤에서의 합의에도 불구하고, 신용정보법에서는 제2조 17호에서 '익명처리'의 개념을 포함하였다. 그런데 이와 같은 개념 체계를 GDPR로부터 차용했음에도 불구하고, '가명처리' 개념이 활용되는 맥락은 GDPR과 사뭇 차이가 존재한다.

개정 개인정보 보호법 제2조 1의2호는 '가명처리'에 대한 정의를 "개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다"고 규정하고 있다. 제2조 1호 개인정보의 정의에서는 다목에서 "가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보"를 가명정보로 규정하고 있는데, 가명정보를 개인정보의 하위 규정으로 둠으로써 가명정보가 개인정보임을 명확히 하고 있다. GDPR에서는 제4조 5호에서 "가명처리는 추가적인 정보의 사용 없이는 더 이상 특정 개인정보주체에게 연계될 수 없는 방식으로 개인정보를 처리하는 것이다. 단, 그 같은 추가 정보는 별도로 보관하고, 기술 및 관리적 조치를 적용하여 해당 개인정보가 식별된 또는 식별될 수 있는 자연인에 연계되지 않도록 해야 한다"고 규정하고 있으며, 전문에서 가명처리된 개인정보 역시 개인정보로 간주되어야 한다고 설명하고 있다[134].

그런데 GDPR은 가명정보를 정의하고 있지는 않다. 유럽기본권청이 발간한 <유럽의 개인정보 보호 법률 핸드북>에서는 유럽의 법률에는 '가명정보(pseudonymised data)'라는 개념이 없다고 설명하고 있다[135]. 이는 가명처리의 방법이 정해져 있는 것이 아니라 다양한 방식과 수준의 가명처리가 가능하고 이에 따라 가명처리의 결과물도 다양할 수

134) GDPR 전문 26.
135) There is no concept of 'pseudonymised data' under EU law. FRA(2018a) p83.

있는데, 가명정보라고 규정하는 순간 ‘고정된 어떤 것’을 의미하는 것으로 해석될 위험이 있기 때문으로 보인다. 즉, 유럽에서는 가명정보라는 특정한 상태가 아니라, 개인정보 침해 위험을 줄이기 위한 ‘안전조치’로서 가명처리를 인식하고 있다. 이러한 안전조치는 가명처리만 있는 것이 아니며, 가명처리가 개인정보 보호를 위한 다른 안전조치를 배제하려는 것은 아니다[136]. 가명처리는 GDPR의 여러 조문에서 안전조치의 하나로 포함되어 있다. 예를 들어, GDPR 제6조 제4항에서 개인정보의 목적 외 처리가 해당 개인정보를 수집한 당초 목적과 양립될 수 있는지 확인하기 위해서 고려해야 할 사항 중의 하나로 ‘암호처리나 가명처리 등 적절한 안전조치의 존재’를 들고 있으며, 제25조(설계 및 기본설정에 의한 개인정보 보호) 제1항에서는 개인정보의 처리 방법을 결정한 시점 및 그 처리가 이루어지는 해당 시점에 가명처리 등 기술적, 관리적 조치가 이행되어야 함을 규정하고 있다.

한국의 개정 개인정보 보호법은 제3절 가명정보의 처리에 관한 특례에서 관련 조항들을 신설하여 가명정보의 활용 방법을 집중적으로 규정하고 있다. 제28조의2는 “통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있”도록 하고 있으며, 제28조의3은 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관을 통해 “서로 다른 개인정보처리자 간의 가명정보의 결합”을 수행하도록 하고 있다. 제28조의4는 가명정보를 처리하는 경우에도 일정한 안전조치를 취하도록 하고 있는데, 제1항에서는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하도록 하고 있으며, 2항에서 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 관련 기록을 작성하여 보관할 것을 의무화하고 있다. 제28조의5는 가명정보의 재식별을 금지하고 있으며 제28조의6은 재식별 금지 의무 위반시 과징금을 부과함을 규정하고 있다. 그리고 제28조의7은 수집출처 고지(제20조), 개인정보 파기(제21조) 등 일부 조항의 적용을 가명정보에 대해 배제하고 있다.

우선 제3절 가명정보 처리에 관한 특례 조항의 입법상의 결함에 대해 지적할 필요가 있다. 제3절은 ‘가명정보의 처리’라는 표현을 쓰고 있지만, 가명처리와 가명정보의 처리는 다르다. 가명처리는 법 제2조 1의2호에서 규정하고 있는 바와 같이 “개인정보의

136) GDPR 전문 28.

일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것”을 말하며, 가명정보의 처리는 이미 가명처리된 개인정보를 처리한다는 의미이다. 제28조의2는 “통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다”고 하고 있지만, 사실 입법자의 의도는 가명처리를 포함하는 것으로 보인다. 그런데 제28조의2는 ‘가명정보의 처리’만을 언급하고 있기 때문에 문언 그대로 엄격하게 해석을 한다면, 과학적 연구 등의 목적을 위해 이미 가명처리된 개인정보를 처리하는 것은 가능하지만, 가명처리 자체를 할 근거는 없다. 가명처리 자체는 정보주체의 동의를 받거나 법령에 근거하여 처리하는 등의 다른 규정에 의존할 수밖에 없는 것이다. 그러나 입법 의도가 그렇지 않기 때문에 개인정보 보호위원회가 문언 그대로 해석하지는 않을 것이며, 제28조의2가 가명처리를 포함하는 것으로 해석할 것이다. 그런데 이렇게 되면, 가명처리와 가명정보의 처리가 다름에도 불구하고 이를 같은 것으로 해석함으로써 관련된 여러 규정에 혼란을 야기할 수밖에 없다. 예를 들어, 제28조의7은 가명정보에 대해 정보주체의 열람권을 배제하고 있는데 가명처리에 대해서도 열람권을 배제하는 것인지가 문제가 될 수 있는 것이다. 당장은 하위 규범이나 해설서를 통해 관련한 해석을 제시할 수밖에 없겠지만, 이러한 혼란을 해결하기 위해서는 법 개정을 통해 명확하게 규정할 필요가 있다.

이와 같은 해석상의 문제점과 별개로, 한국의 개정 개인정보 보호법에서 가명처리 개념이 활용되는 맥락은 GDPR과 다르다. 전술하였듯이, GDPR에서는 안전조치의 하나로서 가명처리를 인식하고 있으며, 개인정보를 목적 외로 활용하든 그렇지 않든, 개인정보의 가명처리가 가능하다면 하는 것이 좋다. 왜냐하면 개인정보를 더 안전하게 관리할 수 있기 때문이다. 반면, 국내 개인정보 보호법은 당초 수집 목적 외 처리를 위한 조건으로 가명처리를 인식하고 있다. 즉, 가명처리를 하면 개인정보 침해의 위험성이 적어지므로 자유롭게 활용할 수 있는 조건이 성립된 것처럼 인식하는 것이다. 결국 개인정보의 목적 외 활용을 합리화하기 위해 ‘가명처리’ 개념을 도입한 것이다. 인재근 의원안은 ‘제안이유’에서 “안전하게 데이터를 활용하기 위한 방법과 기준 등을 새롭게 마련하여 데이터를 기반으로 하는 새로운 기술·제품·서비스의 개발 등 산업적 목적을 포함하는 과학적 연구, 시장조사 등 상업적 목적의 통계작성, 공익적 기록보존 등의 목적으로도 가명정보를 이용할 수 있도록” 하는 것을 목적으로 함을 밝히고 있다.

이와 같은 가명처리에 대한 인식의 차이는 실제 개인정보 처리 과정의 차이를 야기할 수 있다. 과학적 연구 목적의 개인정보 처리를 예로 들어보자. 과학적 연구가 수행되는 맥락은 다양할 수 있는데, 예를 들어 정보주체의 동의를 받아서 수행할 수도 있고, 공공기관의 업무로써 수행될 수도 있으며, 대학의 연구진이 학술 연구의 하나로 수행할 수도 있다. 어떤 경우이든 유럽의 개인정보처리자는 자신이 과학적 연구 목적으로 개인정보를 처리할 때 제6조에서 규정하고 있는 적법성(Lawfulness of processing) 요건 중 어떠한 요건에 따라 처리를 하는 것인지 명확하게 할 필요가 있다. 또한 모든 개인정보 처리는 제5조의 개인정보 처리원칙을 준수해야 하는데, 개인정보는 “구체적이고 명시적이며 적법한 목적을 위해 수집되어야 하고, 해당 목적과 양립되지 않는 방식으로 추가 처리되어서는 안 된다.” 다만, “제89조(1)에 따른, 공익적 기록보존의 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적을 위한 추가 처리는 본래의 목적과 양립되지 않는 것으로 보지 않는다.” 즉, 애초 수집 목적과 달라도 과학적 연구 목적으로 처리할 수 있는데, 이 경우 89조의 1항을 준수해야 한다. 89조의 1항은 과학적 연구 등의 목적으로 처리될 때 데이터 최소화 원칙을 보장하기 위한 기술적, 조직적 조치 등 안전조치를 취하도록 하는데, 가명처리 역시 안전조치에 해당할 수 있다. 만일 익명처리로도 과학적 연구 목적을 달성할 수 있다면 가명처리가 아니라 익명처리하도록 하고 있다. 다시 정리하자면 유럽연합에서 과학적 연구는 사안에 따라 동의, 가명처리, 익명처리 등에 기반하여 수행될 수 있고, 과학적 연구를 수행하는 컨트롤러는 제6조에 따른 적법성 요건을 갖추어야 하며, 해당 연구 목적을 달성하면서도 개인정보 침해를 최소화할 수 있는 비례적인 조치를 취해야 한다.

반면, 국내 개인정보 보호법 제28조의2는 “개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다”고 규정하여 마치 가명처리만 하면 정보주체의 동의 없이 과학적 연구 목적으로 사용할 수 있는 것처럼 규정하고 있다. 그 자체로 원래의 개인정보를 보유하고 있는 개인정보처리자뿐만 아니라 가명정보를 제공받는 제3자 개인정보처리자 역시 별도의 적법성 요건을 갖출 필요 없이 과학적 연구 목적으로 활용할 수 있도록 하고 있다.

또한, 과학적 연구를 위해 익명처리된 개인정보를 활용하는 것으로 충분할 경우 익명처리를 해야 하는지, 아니면 가명처리만 해서 활용해도 되는지도 모호하다. 법 제3조에

서 “개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집 목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다”고 규정하고 있기 때문에, 특정 과학적 연구를 위해 굳이 가명처리된 정보가 아니라 익명처리된 정보로도 충분하다면 익명처리해야한다고 해석하는 것이 옳을 것이다. 그러나 제28조의2만을 보자면 가명정보로 처리해도 법적인 문제가 없는 것으로 해석될 수도 있다. 또한 제28조의4에서 가명정보를 사용할 경우에도 필요한 기술적·관리적 및 물리적 조치를 하도록 의무화하고 있기는 하지만, 이는 “해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록” 하는 보안조치에 가까우며 과학적 연구에 활용되는 데이터를 최소화하는 등의 제반 정책까지 포함하는지는 명확하지 않다.

다. 과학적 연구의 범위

1) 과학적 연구란 무엇인가?

개인정보 보호법 개정 과정에서 가장 논란이 되었던 이슈 중 하나가 과학적 연구의 범위였다. 개정 개인정보 보호법은 제2조 8호에서 과학적 연구를 “기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구”로 정의하고 있으며, 제28조의2에서 개인정보처리자가 ‘통계작성, 과학적 연구, 공익적 기록보존’ 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있도록 하고 있다. 또한 제28조의3에서는 ‘통계작성, 과학적 연구, 공익적 기록보존’ 등을 위해 서로 다른 개인정보처리자간 가명정보의 결합을 전문기관을 통해 수행할 수 있도록 하였다. 그런데 법에서 통계나 공익적 기록보존이 무엇인지에 대해서는 따로 정의하지 않았다.

개정 이전의 기존 개인정보 보호법에는 제18조 2항 4호에 유사한 규정이 있었다. “통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우” 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있도록 허용한 것이다. 학술연구에 대한 별도의 정의는 없었다. 이 규정을 현행 제28조의3으로 대체하면서 과학적 연구로 개념을 바꾸고 정의 규정을 둔 것이다.

전술한 바와 같이 이와 관련된 논란은 2018년 대통령산하 4차산업혁명위원회가 주최한 규제·제도혁신 해커톤에서부터 시작된 것이다. 2018년 4월 3-4일 개최된 제3차 규제·제도혁신 해커톤에서는 '가명정보의 활용 목적과 범위'에 대해 논의하였지만 이해관계자간 합의에 이르지는 못하였다. 의제별 토론 결과를 보면 "가명정보는 ① 공익을 위한 기록 보존의 목적, ② [학술 연구 / 학술 및 연구] 목적, ③ 통계 목적을 위하여 당초 수집 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다고 합의"하였다고 하는데, [학술 연구 / 학술 및 연구]라는 표현은 참석자 간에 이견이 있었음을 보여준다. 즉, 시민사회는 '학술 연구'를, 산업계는 '학술 및 연구'를 주장한 것이다. 산업계 요구는 통상적인 학술 연구를 넘어 기업 내부에서 수행되는 산업적인 연구로 가명정보의 활용 범위가 확대되어야 한다는 것이다. 사실상 정부안이라고 볼 수 있는 인재근 의원 대표 발의 개인정보 보호법은 산업계의 의견을 수용한 것인데, 이를 위해 굳이 기존 법률에 학술 연구라는 개념을 사용하고 있었음에도 과학적 연구로 개념을 변경하였다. 인재근 의원안은 '제안이유'에서 "데이터를 기반으로 하는 새로운 기술·제품·서비스의 개발 등 산업적 목적을 포함하는 과학적 연구, 시장조사 등 상업적 목적의 통계작성, 공익적 기록보존 등의 목적으로도 가명정보를 이용할 수 있도록" 하겠다는 취지를 포함하여 산업계의 주장을 수용했음을 명확히 하였다.

이처럼 과학적 연구의 개념 범위를 규정한 취지 역시 인재근 의원안의 '제안 이유'에서 찾아볼 수 있다. 즉, "4차 산업혁명 시대를 맞아 핵심 자원인 데이터의 이용 활성화를 통한 신산업 육성이 범국가적 과제로 대두되고 있으며, 특히 신산업 육성을 위해서는 인공지능(AI), 클라우드, 사물인터넷(IoT) 등 신기술을 활용한 데이터 이용이 필요"하다는 것이다. 빅데이터, 인공지능 기술의 개발을 위해서는 수천만 건의 데이터 처리가 필요한데 일일이 정보주체의 동의를 받기 힘드니 동의 없이 처리할 수 있도록 하되, 가명처리를 통해 개인정보 침해 위험성을 낮추겠다는 취지다. 물론 익명처리할 경우 개인정보 보호법의 적용을 아예 배제할 수 있지만, 개인정보의 식별성을 익명정보 수준으로 떨어뜨릴 경우 데이터의 가치가 떨어지기 때문에 산업계는 선호하지 않는다. 근본적으로 데이터의 가치와 개인정보 침해 위험성 사이의 긴장이 내재해 있는 것이다.

시민사회는 빅데이터나 인공지능 기술의 개발에 반대하는 것은 아니지만, 정보주체의 동의 없는 개인정보의 목적 외 활용은 '학술연구'로 제한되어야 한다고 본다. "누군

가 자신의 행위를 ‘연구’라고 지칭한다고 무조건 허용하는 것이 아니라, 과학적 방법을 사용하고 과학적 가치가 있는 것이어야” 하며, “연구 결과물의 공개 등을 통한 과학적, 기술적 기반 확대라는 사회적인 기여가 인정되어야” 한다는 것이다. 왜냐하면, “학술 연구나 통계작성을 위해 일정하게 정보주체의 권리를 제약하는 것은 그에 상응하는 사회적인 가치와 기여가 있기 때문”이며, 순전히 사적인 이익을 위한 개인정보 활용을 위해 정보주체의 권리를 제한해야 할 이유가 없다는 것이다[137].

헌법적 관점에서 보면, 국민의 모든 자유와 권리는 국가안전보장·질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률로써 제한할 수 있다(헌법 제37조 제2항). 이에 비추어보면, 개인정보 보호법에서 통계작성 등을 위해 개인정보의 목적 외 이용 혹은 제3자 제공을 허용하더라도, 개인정보 자기결정권이라는 헌법상 제한되는 기본권보다 우월한 공익이 존재하는 경우라야 기본권에 대한 침해가 정당화될 수 있다. 따라서 기본권의 제한과 이로 인해 달성할 수 있는 공익 사이의 비교형량이 필요하다. 전체 국민이 아니라 일부의 특정 사인(私人)의 이윤 창출을 위한 상업적 목적 통계작성이나 산업적 연구를 위한 경우에까지 정보주체의 동의권을 일률적으로 박탈하는 것은 충돌하는 법익 간의 균형을 고려하지 아니하는 결과가 될 수 있다[138].

신용정보법에서는 “통계작성, 연구, 공익적 기록보존 등을 위하여 가명정보를 제공하는 경우” 신용정보회사등이 개인신용정보를 정보주체의 동의 없이 제공할 수 있도록 하면서, 아예 법에서 “이 경우 통계작성에는 시장조사 등 상업적 목적의 통계작성을 포함하며, 연구에는 산업적 연구를 포함한다”고 명시하고 있다(제32조 제6항 9의2).

그런데 사실 ‘상업적 목적의 통계작성’ 및 ‘산업적 연구’를 포함한다는 의미는 다양하게 해석될 수 있다. 즉, 과학적 연구 중 산업적 연구가 일부 있을 수 있다는 의미가 될 수도 있고, 과학적 연구에 산업적 연구가 모두 포함된다는 의미가 될 수도 있다. 산업계가 요구하는 것은 후자일 것이다. 시민사회의 경우 ‘학술 연구’ 혹은 사회적인 가치를 가지는 과학적 연구로 제한해야한다고 주장하고 있는데, 이는 산업적 연구를 모두 포함해야 한다는 산업계의 주장과는 배치되는 것이지만, 일부 산업적 연구의 포함을

137) 건강과대안 외, 2018.11.21., “개인정보보호법 개정안(인재근 의원 대표발의)에 대한 의견”, <https://act.jinbo.net/wp/40024/>.

138) 양기진(2019), 개인정보의 통계작성·연구 목적 활용에 관한 검토- GDPR의 관점상 김병욱 의원 대표발의 개정안의 비판적 검토를 중심으로 -, 법조 제68권 제5호(통권 제737호), p416.

배제하는 것은 아니다. 왜냐하면 학술 연구 역시 산업적 가치나 효용을 가질 수 있기 때문이다. 따라서 시민사회의 주장을 수용하더라도 산업적 연구가 전혀 불가능한 것은 아니다. 그럼에도 불구하고, 개정 개인정보 보호법 통과 이후 발표된 시행령 및 고시 등에서는 과학적 연구의 개념이나 요건을 더욱 구체화하지는 않고 있다. 즉, 현재로서는 과학적 연구라고 주장하는 모든 연구에 열려있는 상황이며, 다만 관련 법적 분쟁을 통한 법원의 해석이나 유럽연합에서 과학적 연구에 대한 보다 세분화된 지침의 등장에 따라 향후 개념이 구체화할 가능성도 있다.

2) GDPR에서 과학적 연구의 의미

이와 관련하여 유럽연합에서의 해석과 관행을 살펴볼 필요가 있다. 한국 정부는 GDPR 적정성 결정을 위한 협상을 진행하고 있는데, 유럽연합과의 무역 관계를 고려한다면 한국의 개인정보 보호 수준이 유럽연합에 상응함을 지속적으로 입증할 필요가 있고, 또 국내 개인정보 보호 규범을 국제적인 규범에 맞춰가는 것이 국내 수범자의 부담도 줄일 수 있기 때문이다.

개정 개인정보 보호법의 과학적 연구의 정의(제2조 8호)의 일부 표현은 GDPR 전문에서 차용한 것이다. 과학적 연구와 관련하여, GDPR은 제5조 개인정보 보호 원칙에서 목적 제한의 원칙을 규정하면서, 다만 공익적 기록보존의 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적을 위한 추가 처리는 본래의 목적과 양립되지 않는 것으로 보지 않는다고 규정하고 있으며, 제89조에서는 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적을 위한 처리와 관련한 안전조치 및 권리 제한을 규정하고 있다. 그러나 GDPR은 과학적 연구(scientific research)에 대한 정의를 별도로 두고 있지 않다. 다만, 전문 159에서 과학적 연구와 관련한 해설을 제공하고 있는데, “과학적 연구 목적의 개인정보 처리는 기술의 발전과 실증, 기초연구, 응용연구 및 민간 투자 연구 등을 포괄하는 광범위한 방식으로 해석”되며, “유럽연합 기능에 관한 조약(TFEU) 제179조에 따라 유럽 연구 영역(European Research Area, ERA)을 구축하려는 유럽연합의 목적이 고려되어야 한다”고 하고 있다. TFEU 제179조 제1항은 연구자, 과학적 지식, 기술이 자유롭게 유통되는 유럽 연구 영역을 구축하고 그것이 더 경쟁적이 되도록 촉진함으로써 과학적, 기술적 기반을 강화하는 것을 유럽연합의 목적으로 설정하고 있다. 2항에

서는 이러한 목적을 위해 유럽연합은 사업체, 연구센터, 대학 등이 높은 수준의 연구 및 기술 개발 활동을 할 수 있도록 촉진하고 그들 사이의 협력 노력을 지지할 것을 규정하고 있다.

종합하면 과학적 연구는 특정 분야, 혹은 공공기관이나 대학 등 특정 기관이 수행하는 연구로 제한되지는 않는다. 동시에 유럽 연구 영역이라는 공통의 지적 공동체에 대한 기여를 고려하도록 하고 있다. 산업적인 연구 혹은 기업이 수행하는 연구를 배제하지는 않지만, '연구'라고 자칭하는 모든 연구로 확대하고 있는 것은 아니다. 전술했듯이 유럽연합의 모든 개인정보처리자는 자신의 개인정보 처리가 GDPR 제6조의 어느 요건에 해당하는지 규정할 필요가 있으며 과학적 연구라면 그 필요성 및 비례성에 맞는 안전조치를 취해야 한다는 점도 고려할 필요가 있다. 즉, 연구의 성격과 가치, 개인정보 침해의 위험성 등의 여러 조건에 따라 취해야 할 안전조치나 적법성 판단 기준이 달라질 수 있다.

아직 유럽연합 내에서도 과학적 연구 목적의 활용에 적용할 개인정보 보호 규범에 대한 구체적인 지침이 나온 것은 아니다. 유럽개인정보보호감독관(European Data Protection Supervisor, EDPS)이 2020년 1월에 발표한 <과학적 연구와 개인정보 보호에 관한 예비 의견서>[139]는 유럽연합에서도 국내와 유사한 고민과 논의가 진행되고 있음을 보여준다. EDPS는 유럽연합 기구의 개인정보 보호를 규율하는 2018/1725 규정에 근거한 감독기관이지만, 이 규정과 GDPR은 크게 다르지 않기 때문에 EDPS의 예비 의견서는 GDPR의 관련 논의에 고려될 수 있고, EDPS 역시 이 의견서가 보다 진전된 논의에 도움이 될 것을 기대하고 있다.

EDPS는 과학적 연구의 개념을 검토하면서 "개인정보처리자가 단지 과학적 연구 목적이라고 주장하는 것으로는 충분하지 않"으며, 학술 연구자(academic researcher)나 비영리 단체 및 정부 기관, 영리 기업도 과학적 연구를 수행할 수 있지만, "과학적 연구가 전체 사회에 유용하며 과학적 지식이 촉진되고 지원해야 할 공공재라는 점을 공통된 전제로 한다"고 보고 있다. 이어 과학적 연구를 위한 개인정보 보호 체계는 다음과 같은 세 가지의 기준이 충족될 경우 적용된다고 규정하고 있다. 첫째 개인정보가 처리될 것, 둘째 정보에 기반한 동의(informed consent), 책임성, 감독의 개념을 포함하여, 관련 분야

139) EDPS(2020), A Preliminary Opinion on data protection and scientific research.

의 방법론이나 윤리가 적용될 것, 셋째 연구가 주로 사적인 이익이 아니라 사회 전체적인 지식 및 복리의 향상을 목적으로 수행될 것 등이다[140]. 또한 GDPR 제5조의 규정이 통계작성이나 역사적, 과학적 연구는 애초 수집 목적과 다르더라도 무조건 양립 가능한 것으로 전제되는지에 대해, 그러한 목적으로 처리하는 것을 무조건 허용하는 것은 아니라고 본다. 그래서 과학적 연구 목적 등으로 활용하기 전에 제6조 4항에 따른 양립가능성 조건을 검토할 필요가 있다고 보고 있다[141].

향후 개인정보보호이사회(EDPB)에서 과학적 연구와 관련하여 보다 구체적인 해석 및 지침을 제공할 것으로 예상된다. 그러나 국내에서도 향후 EDPB의 지침을 따라갈 것이 아니라면, 과학적 연구의 범위에 대해 개인정보 보호위원회의 주도로 다양한 이해관계자 사이의 토론을 진행할 필요가 있다.

3) 과학적 연구 및 통계작성의 주체는 누구인가

제28조의2 제1항은 “개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다”고 규정하고 있다. 여기서 가명정보를 처리하는 주체는 애초에 원래의 개인정보를 보유하고 있는 개인정보처리자로 보인다. 예를 들어, A 통신사가 고객정보를 보유하고 있을 경우, A 통신사의 과학적 연구나 통계작성을 목적으로 고객의 동의 없이 가명처리하여 활용할 수 있다는 것으로 이해된다.

그런데 제2항은 “개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다”고 규정하고 있는데, 여기서 과학적 연구는 누구의 연구를 말하는 것인지 모호하다. 예를 들어, A 통신사의 과학적 연구를 A 통신사가 직접 수행하지 않고 대학의 어떤 교수에 위탁할 수 있다. 이 경우 연구를 실제로 수행하는 것은 교수이지만, 과학적 연구를 수행

140) Ibid., pp11-12.

141) GDPR 6(4)조는 개인정보의 목적 외 처리가 해당 개인정보를 수집한 당초 목적과 양립될 수 있는지 확인하기 위해서 특히 다음 각 호를 고려하도록 하고 있다. (a) 수집 목적과 의도된 추가처리 목적 간의 연관성, (b) 특히 개인정보주체와 컨트롤러 간의 관계와 관련해서 등의 개인정보가 수집된 상황, (c) 특히 제9조에 따른 특정 범주의 개인정보가 처리되는지 여부 또는 제10조에 따른 범죄경력 및 범죄행위와 관련한 개인정보가 처리되는지 여부 등 개인정보의 성격, (d) 의도된 추가처리가 개인정보주체에 초래할 수 있는 결과, (e) 암호처리나 가명처리 등 적절한 안전조치의 존재.

하는 주체는 A 통신사 혹은 A 통신사와 교수 모두라고 볼 수 있다. 그런데 만일 A 통신사가 B 금융사의 과학적 연구를 위해 자신의 고객정보를 가명처리하여 제공하는 경우, 사실 과학적 연구를 수행하는 주체는 B 금융사일 뿐이며, A 통신사의 입장에서 개인정보 처리의 목적은 과학적 연구라기보다는 개인정보의 판매 혹은 제공에 불과하다. 그렇다면 A 통신사 입장에서 자신의 고객정보를 동의 없이 가명처리하여 B 금융사에 제공할 때 제28조의2를 근거로 할 수 있는지 문제가 될 수 있다. 이와 같은 해석상 모호함은 향후 법적 분쟁을 야기할 수 있다.

GDPR의 경우에도 이를 구분하는 조항이 있는 것은 아니다. 그러나 앞서 언급했듯이, GDPR은 개별 처리자마다 자신이 개인정보를 처리하기 위한 정당성을 제6조에서 규정하고 있는 여러 근거 중 하나에 기반하고 있음을 입증할 수 있어야 한다. GDPR에서 타인의 과학적 연구를 목적으로 자신이 보유하고 있는 개인정보를 제공하는 것 역시 애초 수집 목적과 양립하는 것으로 볼 수 있을지 의문이다. 유럽연합에서 이를 어떻게 처리하는지도 지켜볼 필요가 있다.

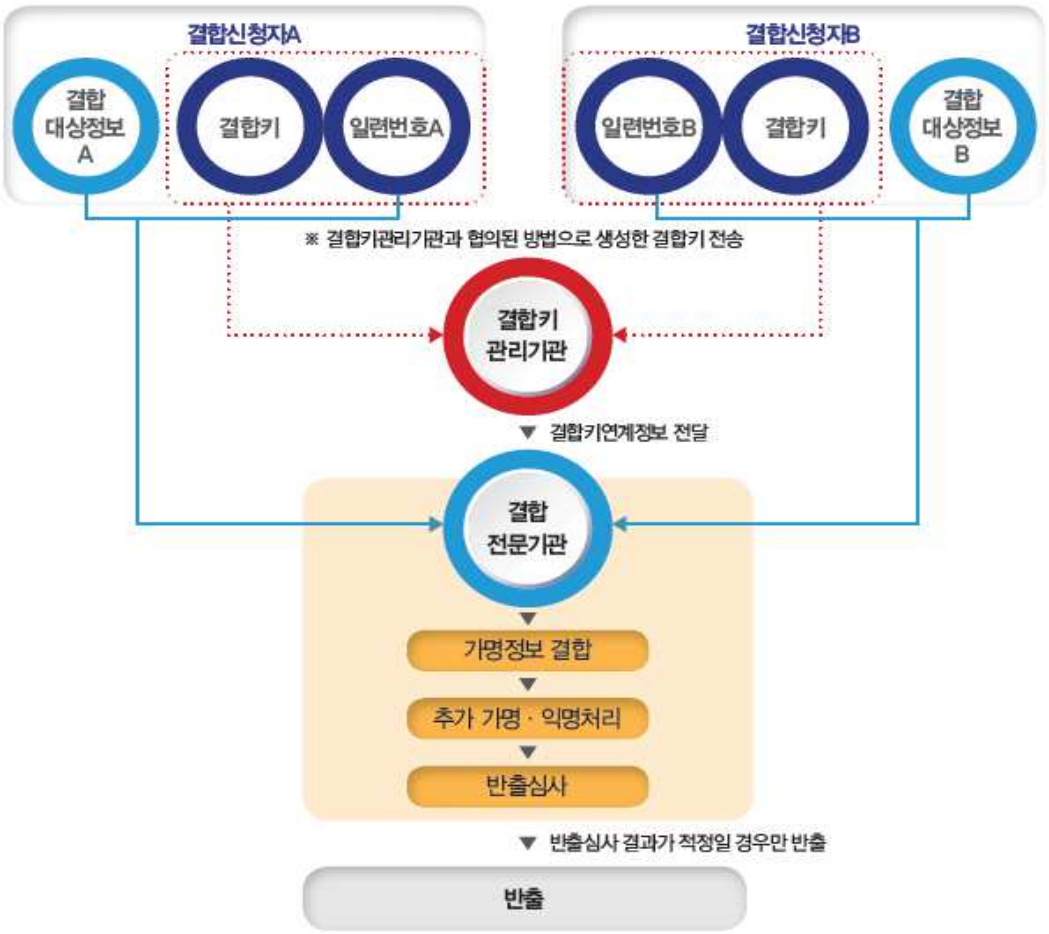
라. 가명정보의 결합

2016년 <개인정보 비식별 조치 가이드라인> 당시부터 큰 논란의 대상이 되었던 이슈 중 하나가 개인정보의 결합이었다. 전술했듯이, 2017년 11월 시민사회단체들은 고객정보 3억4천여만건을 결합한 것에 대해 비식별 전문기관 및 20개 기업을 고발하기도 했다[142]. 제3차 규제·제도혁신 해커톤에서도 데이터 결합의 구체적인 방안에 대해서는 합의에 이르지 못했다. 2019년 3월, 검찰은 위 고발에 관하여 혐의없음(증거불충분)으로 불기소처분하였고[143], 개정 개인정보 보호법은 제28조의3을 통해 전문기관을 통한, 서로 다른 개인정보처리자 간의 가명정보 결합을 허용하고 있다.

제28조의3은 서로 다른 개인정보처리자의 가명정보를 전문기관을 통해 결합하고, 결합된 정보의 반출을 허용한다는 점에서 2016년 <개인정보 비식별 조치 가이드라인>과 큰 틀에서 유사하다. 다만, 2016년 가이드라인에서는 공공기관만을 전문기관으로 지정하였

142) 건강사회를위한약사회 외, 2011.11.9., "시민단체, 고객정보 3억4천여만 건 무단결합한 비식별화 전문기관 및 20개 기업 고발", <https://act.jinbo.net/wp/33555/>.
143) 건강사회를위한약사회 외, 2019.4.1., "정보주체의 동의 없는 개인정보 결합 및 제3자 제공에 면죄부 준 검찰을 규탄한다", <https://act.jinbo.net/wp/40717/>.

<그림3-1> 가명정보 결합, 반출 절차



*출처 : 가명정보 처리 가이드라인(2020)

으나 개정 개인정보 보호법에서는 일정한 요건을 갖추면 개인정보 보호위원회나 관계 중앙행정기관의 장이 민간업체도 전문기관으로 지정할 수 있도록 하였고, 시행령에서 한국인터넷진흥원을 결합키 관리기관으로 지정하여, 결합키를 생성하는 결합키 관리기관과 결합을 수행하는 전문기관의 역할을 구분하였다.

가명정보의 결합은 서로 다른 두 개 이상의 개인정보처리자가 보유하고 있는 개인정보 중 공통된 개인의 속성 정보를 결합한 후, 원 개인정보처리자에게 다시 반출하는 방식으로 이루어진다. 예를 들어, 개인정보처리자 A, B의 고객정보를 결합할 경우, 개인정

보처리자 A는 B와의 공통 고객에 대해 자신이 보유하고 있는 공통 고객의 속성 정보에 더해, B가 보유하고 있던 공통 고객의 속성 정보를 제공받을 수 있는 것이다. 공통 고객의 입장에서는 A, B 두 기업에 각각 제공한 자신의 개인정보를 두 기업이 자신도 모르게 상호 공유하는 결과가 된다.

이에 시민사회단체들은 가명정보 결합에 대해 "기업들에게 고객정보를 판매하고 공유할 수 있도록 하는 것"에 다름 아니라고 비판했다[144] 비록 가명처리를 하더라도 결합된 개인정보는 재식별의 위험성이 높아질뿐더러, 나아가 원래의 개인정보 데이터베이스를 보유하고 있는 개인정보처리자에게는 최소한 기술적으로는 재식별이 쉽게 가능할 수 있기 때문이다.

GDPR에서는 결합(combination)을 개인정보의 처리(processing)의 하나로 규정하고 있을 뿐, 개인정보의 결합에 대해 별도로 규율하고 있지는 않다. 다만 개인정보의 결합도 개인정보의 처리의 하나이기 때문에 제5조의 개인정보 처리원칙, 제6조 처리의 적법성 등 GDPR을 준수해야 한다. 특히 개인정보의 결합은 서로 다른 목적으로 수집된 개인정보 파일, 나아가 두 개 이상의 컨트롤러가 관여되기 때문에, 각각의 처리에 대해 각 컨트롤러는 별도의 적법성 요건을 갖출 필요가 있다. 예를 들어 A와 B 두 개인정보처리자의 개인정보를 결합한다면 A, B 모두 결합이라는 개인정보 처리를 위한 적법성 근거가 필요하다는 것이다.

실제 관행에 있어서 해외에서는 민간기업의 개인정보 결합을 규율하는 법제나 전문기관을 찾아보기는 힘들다. 다만, 보건의료 분야의 개인정보 혹은 공공기관이 보유하고 있는 개인정보의 연구 목적의 활용을 위해 전문기관을 통해 연구자에게 결합, 제공하거나 통계기관이 통계 작성 목적으로 데이터를 결합하거나 보유하고 있는 데이터를 연구자에게 제공하는 사례들을 볼 수 있다[145]. 각 국의 담당 기관마다 데이터의 결합 및 제공 방식에 차이가 있기는 하지만, 개인정보 보호를 위한 데이터 거버넌스 체제를 구축하고 있다.

예를 들어 뉴질랜드 통계청은 마이크로 데이터에 대한 접근에 대하여 '5가지 안전조치' 체제를 규정하고 있는데, 이는 데이터 최소화 원칙 및 가명/익명 처리 등과 관련된

144) 건강과대안 외, 2018.11.21., "개인정보보호법 개정안(인재근 의원 대표발의)에 대한 의견", <https://act.jinbo.net/wp/40024/>.
145) 이은우 외(2017), 앞의 글.

<그림3-2> 뉴질랜드 통합데이터기반(IDI)의 5가지 안전조치 체제

데이터 안전(Safe data)은 물론, 인력 안전(Safe people)[146], 연구 안전(Safe projects)[147], 환경 안전(Safe settings)[148], 결과물 안전(Safe output)[149] 등의 원칙이다.

이러한 데이터 거버넌스 체제는 비단 데이터 결합을 위해서만 필요한 것은 아니다. 데이터 결합이 이루어지지 않고 다만 개인정보를 과학적 연구나 통계 작성 목적으로 연구자에게 제공할 경우에도 기본적으로 이러한 안전조치가 적용된다.

국내 시민사회단체들은 개정 개인정보 보호법의 가명정보의 결합 규정에 대해 반대해 왔지만, 동시에 안전한 결합을 위한 데이터 거버넌스 체제를 구축할 것을 제안하고 있다[150]. 현재의 과학적 연구 및 통계 작성의 범주 하에서 이루어지는 결합에 반대하는 것이지 개인정보의 결합 자체를 반대하는 것은 아니기 때문이다. 사회적 가치가 있는 학술연구에 필요한 개인정보 결합은 필요할 수 있는데, 그 경우에도 개인정보에 대한 안전조치는 필요하다. 그렇기 때문에 과학적 연구의 범위 논란과 별개로, 과학적 연구 목적의 개인정보 제공이나 결합에 필요한 안전조치로서 데이터 거버넌스는 마련될 필요가 있다.

시민사회가 의견서를 통해 제안한 데이터 거버넌스는 ▲ 가명정보 결합이 '통계작성, 과학적 연구, 공익적 기록보존' 등의 목적에 부합하는지 심사하기 위한 기구(가칭 연구평가위원회)를 구성할 것, ▲ 연구자에 대한 교육 및 훈련을 실시할 것, ▲ 결합된 가명정보의 반출이 아니라 안전시설 내 접근을 원칙으로 할 것, ▲ 가명정보 결합 과정에서

146) 연구자에 대한 검증 및 훈련 등
147) 프로젝트의 학술적 가치에 대한 심사, 계약을 통한 안전성 요구 등
148) 전송 및 보관에 있어서의 보안조치 등
149) 연구결과물이 개인정보를 포함하지 않도록 검증
150) 경실련 외, 2020.5.11., "개인정보보호법 및 신용정보보호법 시행령(안)에 대한 시민사회 의견서", <https://act.jinbo.net/wp/42829/>.

데이터 최소화 원칙을 준수할 것, ▲ 결합된 가명정보를 연구 목적 달성 후에 폐기하도록 할 것, ▲ 해당 연구의 목적, 연구의 기간, 연구기관 및 책임자, 결합에 활용된 가명정보를 보유한 개인정보처리자, 결합의 건수 및 사용된 항목 등 관련 정보 일체를 공개하도록 할 것 등이다. 그러나 이러한 시민사회의 요구는 시행령 및 <가명정보의 결합 및 반출 등에 대한 고시>에 반영되지 않았다.

가명정보 결합과 관련된 안전조치도 정부의 애초 계획에서 후퇴하였다. 행정안전부는 2020년 3월 31일 시행령 일부개정안을 입법예고하였는데, 몇 달 후인 7월 14일 시행령 일부개정안을 재입법예고하였다. 그런데 재입법예고된 시행령은 애초에 입법예고된 안보다 개인정보 보호 측면에서 후퇴한 것이었다. 가명정보 결합과 관련해서도 처음 입법예고된 안에서는 결합된 가명정보의 분석을 안전한 '분석공간'에서 수행하는 것을 원칙으로 하였으나, 재입법예고된 안에서는 원칙적으로 결합된 가명정보의 반출을 허용하는 것으로 변경되었다[151].

이는 산업계의 입장을 수용했기 때문인 것으로 보인다. 4월 29일 행정안전부, 방송통신위원회, 금융위원회가 공동 개최한 데이터 3법 시행령 개정안 온라인 토론회를 위해 작성한 토론문[152]에서 한국인터넷기업협회는 개인정보 보호법에 기반한 가명정보 결합과 신용정보법에 기반한 결합의 절차가 서로 달라 수범자에게 시간적·금전적 추가 비용의 발생을 초래함을 비판하면서, "'물리적 조치'를 근거로 결합된 정보의 분석을 결합전문기관 내에 설치된 (물리적) 분석공간으로 한정하게 될 경우, 결합신청기관이 해당 장소 이용을 위해 이동, 대기하는 등 불편이 예상될 뿐만 아니라, 결합신청기관이 목적하는 분석 방법의 활용이 불가능한 상황이 발생할 수 있"다며 분석공간 내에서 결합된 가명정보에 접근하도록 한 정책에 반대한 바 있다. 한국인터넷기업협회가 개인정보 침해 위험을 줄이기 위해 한국인터넷진흥원을 통해 결합키를 생성하도록 한 부분에 대해서는 "전달되는 과정에서 유출·침해 등의 위험이 높아질 우려"를 제기하면서도, 정작 원래의 개인정보를 보유하고 있어 침해의 위험성이 더 높은 가명정보의 반출에 대해서는 개인정보처리자의 편의성을 근거로 지지하는 것은 모순적이라고 할 수 있다.

국가인권위원회는 개인정보 보호법 시행령 일부개정령안에 대한 검토서에서 원칙적으

151) 경실련 외, 2020.7.20., "개인정보 보호법 시행령 일부개정령(안)에 대한 시민사회 2차 의견서", <https://act.jinbo.net/wp/43226/>.
152) 김재환(2020), 토론문- 데이터3법 시행령 개정안 정부 토론회 -.

로 결합전문기관 내 분석공간에서만 결합 가명정보를 분석할 수 있도록 규정한 것은 긍정적이지만, 1) 분석공간에서 결합 목적을 달성하기 어렵거나 2) 분석공간 이용이 어려운 경우에는 예외적으로 반출을 승인할 수 있도록 규정하는데 그러한 경우가 구체적으로 어떠한 경우인지, 단지 '분석공간 이용이 어려운' 이유만으로 반출을 허용할 수 있는지에 대해 면밀한 재검토가 필요하다고 지적하며, "가명 결합정보의 구체적 반출요건을 전면 재검토하고, 고시가 아닌 시행령에 구체적으로 규정할 것"을 권고하였다. 또한 법 및 시행령에서 외부 반출된 결합가명정보가 금전적 대가를 받고 판매·거래되는 행위를 금지하는 명시적 규정을 두고 있지 않다며, 이를 명시적으로 금지하는 규정을 보완할 것을 권고하였다[153]. 그러나 이와 같은 국가인권위원회의 의견도 최종 시행령에 수용되지 않았다. 가명정보의 결합 지원은 전 세계적으로 유사한 사례를 찾아보기 힘든 정책으로, 개인정보 침해 위험성에도 불구하고 산업계의 요구를 수용한 대표적인 정책이라고 평가할 수 있다.

마. 정보주체의 권리 제한

개정 개인정보 보호법 제28조의7은 가명정보에 대해 제20조, 제21조, 제27조, 제34조제1항, 제35조부터 제37조까지, 제39조의3, 제39조의4, 제39조의6부터 제39조의8 규정의 적용을 배제하고 있다. 열거된 조항의 적용을 배제하는 이유는 해당 조항을 적용하기 위해서는 가명정보를 재식별해야 하고 이는 오히려 가명처리를 한 취지에 반한다는 이유일 것으로 보인다.

<가명정보에 대해 적용되지 않는 조항>

제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지)
제21조(개인정보의 파기)
제27조(영업양도 등에 따른 개인정보의 이전 제한)
제34조(개인정보 유출 통지 등) 제1항
제35조(개인정보 열람)
제36조(개인정보의 정정·삭제)
제37조(개인정보의 처리정지 등)
제39조의3(개인정보의 수집·이용 동의 등에 대한 특례)

153) 국가인권위원회(2020), 개인정보 보호법 시행령 일부개정령안 검토서.

제39조의4(개인정보 유출등의 통지·신고에 대한 특례)
제39조의6(개인정보 보호조치에 대한 특례)
제39조의7(이용자의 권리 등에 대한 특례)
제39조의8(개인정보 이용내역의 통지)

우선 이 조항은 '가명정보'에 대해 적용됨을 인식할 필요가 있다. 즉, '가명처리'에는 적용되지 않는다. 예를 들어, 제35조에서 규정하고 있는 정보주체의 자기 정보에 대한 열람권의 경우, 제28조의7에 따라 이미 가명처리된 정보에 대한 정보주체의 열람권은 보장되지 않지만, 자신의 개인정보를 가명처리했는지 여부에 대한 열람권은 보장된다는 것이다. 원래 인재근 의원이 대표 발의한 개인정보 보호법 개정안은 제28조의7 제1항에서 가명정보에 대해 일부 조항에 대한 적용 배제를 규정하고, 제2항에서는 가명처리에 대한 일부 조항의 적용 배제를 규정하고 있었으나 국회 심사 과정에서 제2항은 삭제되었다. 따라서 가명처리에 대해서는 정보주체의 권리를 제한하지 않고자 하는 것이 입법자의 의도라고 볼 수 있다.

그러나 제28조의7 조항의 타당성에 대해서는 몇 가지 문제를 제기할 수 있다. 우선 제28조의7과 같이 정보주체의 권리에 해당하는 특정 조항을 무조건 적용 배제하는 방식이 타당한지 의문이다. 가명정보를 처리하더라도 항상 정보주체의 권리 보장이 불가능하거나 혹은 그 권리를 보장하는 것이 정보주체에게 해를 미치게 되는 것은 아니기 때문이다. 예를 들어 가명정보의 일부가 아니라 전부가 유출되었을 경우, 가명처리를 했던 개인정보처리자는 별도로 보관된 추가정보를 통해 누구의 개인정보가 가명처리되었는지 확인할 수 있다. 비록 가명처리되었다고 하더라도 유출된 가명정보가 개인정보 침해 위험이 크다면 해당 정보주체에게 통지를 할 필요가 있으며, 이것이 정보주체에게 해를 입히는 것도 아니다. 혹은 특정한 정보주체가 자신의 개인정보를 처리하지 말아달라고 요청했을 경우, 원 개인정보처리자는 추가정보를 통해 가명처리된 정보의 대체식별자가 무엇인지 확인할 수 있으며 가명정보 처리자에게 해당 정보의 처리정지를 전달할 수 있을 것이다. 이처럼 가명정보라고 할지라도 정보주체의 권리를 보장하는 것이 현실적으로 불가능하다고 단정하기는 힘들다.

GDPR의 경우 제89조의 2항에서 개인정보가 과학적 또는 역사적 연구 목적이나 통계적 목적으로 처리되는 경우, 유럽연합 또는 회원국 법률에서 규정한 조건 및 안전조치에

따라 제15조 등 일부 권리의 적용을 일부 제한할 수는 있지만, 무조건 해당 조항의 적용을 배제하는 것이 아니라 “정보주체의 권리를 보장하는 것이 특정한 처리 목적의 달성을 불가능하게 하거나 중대하게 손상시킬 것으로 예상되고, 처리 목적을 달성하기 위하여 권리 적용을 일부 제외할 필요”가 있을 때에 한한다. 따라서 국내 개인정보 보호법에서도 GDPR과 마찬가지로 그러한 권리를 보장할 때 과학적 연구 등의 목적 달성을 불가능하게 하거나 손상시킬 우려가 있을 경우에만 권리를 제한하는 방식으로 규정하는 것이 바람직하다.

둘째, 제28조의7은 가명정보에 대해 제21조(개인정보의 파기)의 적용을 배제하고 있는데, 그 의미가 특정한 통계작성이나 과학적 연구 등을 위해 가명처리된 개인정보를 해당 목적이 달성된 이후에도 계속 보관할 수 있다는 것인지 모호하다. 제21조의 적용 배제는 두 가지로 해석될 수 있는데, 통계작성이나 과학적 연구 등의 목적 수행을 위해 애초 수집된 목적이 달성된 이후에도 파기하지 않고 추가 보관할 수 있다는 의미일 수도 있고, 가명정보에 대해서는 제21조에서 규정한 개인정보의 파기 의무를 아예 배제하여 무기한 보관할 수 있다는 의미로 해석될 수도 있다. 목적을 특정하지 않고 개인정보(가명정보 역시 개인정보이다)를 무기한 보관하는 것은 개인정보 보호를 위한 국제규범이나 개인정보 보호법 제3조의 개인정보 보호원칙에 벗어난다는 점에서 전자로 해석하는 것이 타당해 보인다. 그런데 행정안전부는 2020년 7월 14일 재입법예고한 시행령 일부개정안에서 3월 31일 입법예고된 시행령 일부개정안에는 포함되어있었던 제29조의5 제3항을 삭제하였다. 해당 조항은 “가명정보의 처리 목적이 달성되거나 가명정보 보유 기간이 경과한 때에는 그 가명정보를 지체 없이 파기”하도록 하고 있다. 이러한 시행령 조항의 변경이 가명정보의 무기한 보관을 의미하는 것인지에 대해 공식적인 가이드라인이나 해설서 등을 통해 밝혀질 필요가 있는데, 만일 그렇다면 개인정보 보호원칙을 위배했다는 비판에서 자유롭기 못할 것이다.

유럽 개인정보보호감독관(EDPS) 역시 이와 같은 잘못된 해석의 가능성을 지적하고 있다. GDPR 제5조(e)는 보유기간 제한의 원칙(storage limitaion)을 규정하면서 “공익적 기록 보존 목적, 과학적 또는 역사적 연구 목적, 통계적 목적을 위해 처리되는 경우 더 오랜 기간 동안 보관될 수 있다”고 덧붙이고 있다. 이에 대해 EDPS는 “연구 기관들이 GDPR의 특별 조항을 개인정보를 무한정 보관할 수 있도록 허용하는 것으로 해석하거나

정보주체에게 정보를 제공할 권리를 부인하는 것은 개인정보의 남용으로 간주될 수 있다" 고 지적했다[154].

바. 과학적 연구 목적의 민감정보 활용

개정 개인정보 보호법의 '제3절 가명정보의 처리에 관한 특례' 가 제23조 민감정보에도 적용되는지에 대해서 논란이 있을 수 있다. 특히 의료정보를 포함한 개인 건강정보는 개인의 권리에 치명적인 영향을 미칠 수 있는 민감정보이지만, 보건의료 분야의 연구 등 공공적, 산업적 측면에서 활용 가치가 높은 정보로 인식되고 있다. 그런데 이번 개인정보 보호법 개정에 제23조 개정은 포함되지 않았다.

지금까지 민감정보는 원칙적으로 처리가 금지되며 제23조에 근거해서 예외적으로만 처리할 수 있는 것으로 해석되어 왔다. 제23조는 정보주체의 별도 동의가 있거나 법령에서 처리를 요구하는 경우에만 민감정보의 처리를 허용하고 있다. 2016년 12월 발간된 <개인정보 보호법 해설서>에서는 "제23조는 개인정보 처리에 관하여 특별한 규정이므로 제15조, 제17조 및 제18조 등 개인정보 처리에 관한 규정에 우선하여 적용된다. 따라서 민감정보의 경우에는 제23조 제1항 각호에서 정하는 예외 사유가 존재하는 경우에 한하여 처리할 수 있다" 고 설명하고 있다. 따라서 가명정보 역시 개인정보이기 때문에 제23조에 따라 정보주체의 별도 동의나 법령의 근거 없이는 제3절 가명정보의 처리에 관한 특례에 따라 처리할 수 없다고 해석할 수 있다.

그러나 정부는 제3절의 규정이 민감정보에도 적용된다고 해석하고 있다. 2020년 9월 보건복지부와 개인정보 보호위원회가 공동으로 <보건의료 데이터 활용 가이드라인>을 발표한 것으로도 이러한 입장을 알 수 있다. 제23조에도 불구하고 왜 제3절이 적용되는 것으로 해석하는지에 대해 공식적인 설명은 없지만, 제3절이 나중에 신설되었고 제23조 뒤에 나온다는 점이 그러한 법률 해석의 근거인 것으로 보인다.

민감정보 중 개인 의료정보의 경우에는 의료법과의 관계도 논란이 될 수 있다. 개인정보 보호법 제6조는 "개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다" 고 하고 있다. 따라서 의료기관이 보유하

154) EDPS(2020), op. cit., p18.

고 있는 환자에 관한 기록에 대해서는 의료법이 우선 적용된다. 의료법 제21조 제2항은 (3항에서 규정된 경우를 제외하고는) “의료인, 의료기관의 장 및 의료기관 종사자는 환자가 아닌 다른 사람에게 환자에 관한 기록을 열람하게 하거나 그 사본을 내주는 등 내용을 확인할 수 있게 하여서는 아니 된다” 고 규정하고 있다. 가명처리된 개인 의료기록 역시 개인정보라고 본다면 이 조항에 따라 정보주체인 환자의 동의 없이 제3자에게 제공해서는 안 될 것이다. 그런데 <보건의료 데이터 활용 가이드라인>은 가명처리하여 환자식별력이 없는 진료기록에 대해서는 의료법이 아닌 개인정보 보호법이 적용된다고 해석하고 있다[155].

GDPR의 경우 제9조 특별 범주의 개인정보 처리에서 민감정보 처리를 규정하고 있다. GDPR 역시 특별 범주의 개인정보는 원칙적으로 처리가 금지되며 제9조 2항에서 규정한 바에 의해서만 처리할 수 있는데, 제9조 2(j)항은 “추구하는 목적에 비례하고, 개인정보 보호권의 본질을 존중하며, 개인정보주체의 기본적 권리 및 이익을 보호하기 위해 적절하고 구체적인 조치를 제공하는 유럽연합 또는 회원국 법률에 근거하여, 제89조(1)에 따라 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적을 위해 처리가 필요한 경우” 에 민감정보를 처리할 수 있도록 하고 있다. 즉, 과학적 연구 등의 목적을 위해 민감정보의 처리를 허용하되 정보주체의 권리 침해를 방지할 수 있는 충분한 안전조치를 규정하는 별도의 법률에 근거하도록 한 것이다. 영국의 경우 보건의료 개인정보의 연구 목적의 이용을 위해 ‘국가보건서비스법(NHS Act 2006)’의 Section 251에 근거 규정을 두고 있다. 아이슬란드의 경우 건강분야 과학적 연구에 관한 법률(the Act on Scientific Research in the Health Sector, no. 44/2014)을 별도로 두고 있으며, 아일랜드는 건강연구규정 2018(Health Research Regulation 2018)에서 건강연구와 관련된 거버넌스 및 안전조치 등을 구체적으로 규정하고 있다. 물론 건강연구에 대해서는 일반적인 과학적 연구에 비해 더욱 엄격한 안전조치를 요구하고 있다[156].

GDPR 제9조와 비교하면 국내 개인정보 보호법 제23조는 민감정보의 처리를 지나치게 엄격하게 제한하고 있다. 또한 공중보건을 위한 과학적 연구 역시 당연히 필요할 것이다. 그러나 제23조에 명확하게 규정하지 않고 해석에 의해 과학적 연구 목적의 민감정보 처

155) 개인정보보호위원회, 보건복지부(2020), 보건의료 데이터 활용 가이드라인, p34
156) 금융정의연대 외, 2020.2.17., “개인정보보호법 개정 후속 과제에 대한 시민사회 의견서”, <https://act.jinbo.net/wp/42187/>.

리를 정당화하는 것은 바람직하지 않다. GDPR의 경우에는 과학적 연구 목적의 민감정보 처리를 위해서는 별도의 법률적 근거를 요구하는 등 엄격하게 보호하고 있지만, 반대로 국내 개인정보 보호법은 과학적 연구 목적 처리에 있어서 일반적인 정보와 민감정보의 구분이 없는 것처럼 해석하고 있기 때문이다. 이는 민감정보의 처리를 원칙적으로 금지하고 특별히 보호하고자 한 취지를 무시한 것이다. 따라서 국내에서도 제23조에서 별도의 법적 근거가 있을 경우 통계작성 및 과학적 연구 목적의 민감정보 처리가 가능함을 규정하되, 민감정보의 종류에 따라 의료법 등 별도의 법률에서 여타 개인정보의 경우보다 엄격한 안전조치 및 거버넌스 체제를 구체적으로 규정하는 것이 바람직할 것이다.

사. 개인정보의 추가적인 이용·제공 기준

개정 개인정보 보호법 및 신용정보법은 일정한 범위에서 개인정보를 애초 수집 목적 외로 추가적으로 이용·제공할 수 있도록 허용했다. 개인정보 보호법 제15조 제3항은 “개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다”고 규정하고 있다. 마찬가지로 제17조 제4항은 개인정보의 제공 측면에서 같은 내용을 다루고 있다. 신용정보법의 경우에는 제32조에서 개인신용정보를 제공할 때 정보주체의 동의를 받도록 하고 있는데, ’당초 수집한 목적과 상충되지 아니하는 목적으로 개인신용정보를 제공하는 경우’에는 동의가 면제되며, 이러한 목적을 판단할 때 ▲ 양 목적 간의 관련성, ▲ 신용정보회사등이 신용정보주체로부터 개인신용정보를 수집한 경위, ▲ 해당 개인신용정보의 제공이 신용정보주체에게 미치는 영향, ▲ 해당 개인신용정보에 대하여 가명처리를 하는 등 신용정보의 보안대책을 적절히 시행하였는지 여부를 고려하도록 하고 있다. 신용정보법은 동의 없이 개인정보를 활용하기 위해 고려해야 할 요소들을 법에서 규정하고 있는 반면, 개인정보 보호법은 대통령령에 위임하고 있어 시행령 제정 과정에서 논란이 되었다. 왜냐하면, 애초 수집 목적 외로 활용할 수 있는 범위가 어떻게 규정되느냐에 따라 정보주체의 권리나 개인정보의 활용도에 영향을 미칠 수 있기 때문이다.

2020년 3월 31일 입법예고된 개인정보 보호법 시행령 일부개정령(안)은 제14조의2(개인정보의 추가적인 이용·제공 기준 등)를 신설하였는데, 합리적으로 관련된 범위인지에 대한 판단 요소로 다음과 같은 4가지 고려사항을 '모두 충족' 해야 한다고 규정하였다. 첫째 개인정보를 추가적으로 이용하려는 목적이 당초 수집 목적과 상당한 관련성이 있을 것, 둘째 개인정보를 수집한 정황과 처리 관행에 비추어 볼 때 추가적으로 이용할 수 있을 것으로 예측 가능할 것, 셋째 개인정보의 추가적 이용이 정보주체 또는 제3자의 이익을 부당하게 침해하지 아니할 것, 넷째 가명처리를 하여도 추가적 이용 목적을 달성할 수 있는 경우에는 가명처리하여 이용할 것 등이다. 그러나 이 안은 시민사회와 업계 모두의 비판을 받았다.

한국인터넷기업협회는 개정안에 대해, 4가지 사항을 '모두 충족' 하도록 하는 것은 너무 경직되고 엄격한 조건이 설정되어 사업자가 실제 동 조항을 활용하기 어렵고, '상당한' 혹은 '관행' 등 불확정 개념을 사용하는 것은 사업자에게 부담이 되며, 이용자에 대한 부정적 영향뿐만 아니라 긍정적인 영향도 고려되어야 한다고 지적하였다[157]. 시민사회 역시 행정안전부에 제출한 의견서에서, 추가적인 이용·제공의 조건을 엄격하게 규정하지 않으면 개인정보처리자의 자의적인 해석에 따라 개인정보가 애초 수집 목적 외로 무분별하게 활용될 위험성이 있음을 지적하며, 무엇보다 정보주체의 합리적인 기대, 즉 애초의 목적에 비추어 정보주체가 합리적으로 예상할 수 있는 범위를 벗어나지 않도록 해야 한다고 강조했다[158].

그런데 정부는 7월 14일, 시행령 개정안을 재입법예고를 하였다. 재입법예고된 개정안에서 제14조의2 조항의 내용이 다음과 같이 수정이 되었는데, '모두 충족' 이라는 표현과 '상당한' 이라는 표현이 빠지는 등 산업계의 요구를 일부 수용한 것으로 보인다.

애초에 이 조항은 GDPR 제6조 제4항의 규정을 국내에 도입한 것이다. GDPR은 제5조 제1항(b)에서 개인정보를 특정된, 명확하고 적법한 목적을 위해 수집되고, 그 목적과 양립하지 않는 방식으로 추가 처리되어서는 안 된다는 원칙(목적 제한의 원칙)을 규정하고 있다. 제6조 제4항에서는 또 다른 목적이 애초 수집 목적과 양립 가능한지 판단할 때 다음과 같은 사항을 고려하도록 하고 있다. (a) 수집 목적과 의도된 추가처리 목적 간의 연

157) 김재환(2020), 앞의 글, pp2-4.
158) 경실련 외, 2020.5.11., "개인정보보호법 및 신용정보보호법 시행령(안)에 대한 시민사회 의견서", <https://act.jinbo.net/wp/42829/>.

관성 (b) 특히 개인정보주체와 컨트롤러 간의 관계와 관련해서 개인정보가 수집된 상황 (c) 특히 제9조에 따른 특정 범주의 개인정보가 처리되는지 여부 또는 제10조에 따른 범죄경력 및 범죄행위와 관련한 개인정보가 처리되는지 여부 등 개인정보의 성격 (d) 의도된 추가 처리가 개인정보주체에 초래할 수 있는 결과 (e) 암호처리나 가명처리 등 적절한 안전조치의 존재.

그런데 GDPR 원문에서 (a)부터 (e)까지의 고려사항을 열거하면서 'inter alia'라는 용어를 사용한 것을 고려하면, 열거된 조건들을 모두 충족해야 한다거나, 반대로 하나만 충족해도 된다고 해석하는 것은 잘못이며, 개별 사안에 따라 종합적으로 고려하되, 필요하다면 여기 열거되지 않은 상황도 고려할 수 있다고 해석된다.

<표3-2> 두 가지 입법예고안에서 추가적인 이용·제공 기준 내용 비교

시행령(안) - 3월 31일 입법예고안	시행령(안) - 7월 14일 입법예고안
제14조의2(개인정보의 추가적인 이용·제공 기준 등) 법 제15조제3항 및 법 제17조제4항에서 "대통령령으로 정하는 바"란 다음 각 호의 사항을 모두 충족하는 경우를 말한다. 이 경우 법 제17조제4항에 관하여는 '이용'을 '제공'으로 본다. 1. 개인정보를 추가적으로 이용하려는 목적이 당초 수집 목적과 상당한 관련성이 있을 것 2. 개인정보를 수집한 정황과 처리 관행에 비추어 볼 때 추가적으로 이용할 수 있을 것으로 예측 가능할 것 3. 개인정보의 추가적 이용이 정보주체 또는 제3자의 이익을 부당하게 침해하지 아니할 것 4. 가명처리를 하여도 추가적 이용 목적을 달성할 수 있는 경우에는 가명처리하여 이용할 것	제14조의2(개인정보의 추가적인 이용ㆍ제공의 기준 등) ① 개인정보처리자는 법 제15조제3항 또는 법 제17조제4항에 따라 정보주체의 동의 없이 개인정보를 이용 또는 제공(이하 "개인정보의 추가적인 이용 또는 제공"이라 한다)하는 경우에는 다음 각 호의 사항을 고려해야 한다. 1. 당초 수집 목적과 관련성이 있는지 여부 2. 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부 3. 정보주체의 이익을 부당하게 침해하는지 여부 4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 ② 개인정보처리자는 제1항 각 호의 고려사항에 대한 판단 기준을 법 제30조제1항에 따른 개인정보 처리방침에 미리 공개하고, 법 제31조제1항에 따른 개인정보 보호책임자가 해당 기준에 따라 개인정보의 추가적인 이용 또는 제공을 하고 있는지 여부를 점검해야 한다.

이 규정의 취지 및 해석에 대해서는 ‘목적 제한(purpose limitation)’에 대한 29조 작업반의 의견서를 참조할 수 있다[159]. GDPR 제정 이전, 기존 개인정보보호 디렉티브는 제6(1)(b)조에서 목적 제한의 원칙을 규정하고 있었는데, 29조 작업반은 이 원칙에 대한 의견서에서 ’양립 가능성 평가(compatibility assessment)’를 위한 프레임워크를 제시하였다. 이 의견서에서 제시된, 양립가능성 평가를 위한 요소들은 이후 GDPR 제6조 제4항에 반영되었다.

기존 디렉티브 및 GDPR에서 “양립 가능하지 않은 목적으로 추가 처리해서는 안된다”는 방식으로 표현한 것은 처리 목적에 대한 다소 유연한 해석을 의도한 것이다. 즉, 추가 처리의 목적이 애초 수집 목적과 다르다고 해서 자동적으로 양립 가능하지 않은 것은 아니라는 것이다. 이러한 유연성을 부여한 이유는 애초에 개인정보를 수집할 때에 비해서 사회의 기대 혹은 정보주체의 기대가 변화할 수 있는데, 일정한 범위 내에서 애초에 처리자나 정보주체가 생각하지 못했던 목적의 변화를 수용할 필요성이 있기 때문이다. 그래서 몇 가지 요소들을 고려하여 양립 가능성 테스트를 충족하면 양립 가능하지 않은 것은 아니라고 간주하는 것이다.

맥락에 따라 애초 수집 목적과 추가적인 처리 목적의 관계가 다를 수 있기 때문에 개별 사안별로 이러한 판단을 할 수밖에 없다. 예를 들어, 소비자가 판매상에게 자신의 주소와 계좌 정보를 처음 제공한 이후, 매주 물품 배달을 위해 해당 정보를 추가로 처리하는 것은 명확하게 양립 가능한 추가 처리에 해당한다. 그런데 이 판매상이 고객의 이메일이나 구매 목록을 유사 상품에 대한 할인 쿠폰을 주기 위해 활용할 경우, 이것이 양립 가능한 목적인지는 보다 면밀한 분석이 필요해진다. 만일 소비자의 개인정보를 유사 업종의 다른 판매상에게 판매하고자 한다면 양립 가능한 목적에 해당할 가능성이 적어질 것이다. 애초에 동의를 받을 때 할인 쿠폰을 제공하겠다는 목적을 명시하지 않았더라도 할인 쿠폰을 제공하는 것이 정보주체가 합리적으로 기대할 수 있는 범위의 처리라면 오히려 별도의 동의를 해야 하는 정보주체의 부담을 덜어줄 수 있다. 그러나 정보주체의 합리적 기대를 벗어나는 방식으로 추가 처리된다면, 정보주체 입장에서는 자신의 권리를 침해당했다고 느낄 수밖에 없다.

159) ARTICLE 29 DATA PROTECTION WORKING PARTY(2013), Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203.

이 규정은 수집 목적과 다른 목적으로 추가 처리될 가능성을 배제하지 않는다는 점에서 처음부터 권리 침해의 가능성을 내포하고 있다. 개정 개인정보 보호법에 신설된 이 조항이 향후 어떻게 활용이 될 것인지 지켜볼 필요가 있다.

3. 신용정보법을 둘러싼 쟁점

신용정보법과 관련된 가장 큰 쟁점은 개인정보 보호법과의 법제 및 감독 권한의 일원화 문제였다. 데이터 3법의 주요한 개정 목적 중의 하나도 법제 간의 혼란 및 중복을 해소하는 것이었으며, 김병욱 의원이 대표 발의한 신용정보법 개정안 역시 "일반법인 「개인정보 보호법」과의 유사·중복 조항 정비"를 제안 이유의 하나로 규정하고 있다. 그럼에도 불구하고, 앞서 본 바와 같이 개인정보 보호법과 신용정보법은 가명처리의 개념 등 유사한 내용에 대해 서로 다른 개념과 절차를 적용하고 있어 오히려 혼란을 야기하고 있다.

한편, 신용정보법에 대해서도 가명처리한 개인신용정보의 연구 목적 활용 및 연계와 관련한 논란이 제기된다. 이는 개인정보 보호법에서의 논란과 다르지 않으므로 여기서 자세하게 다루지는 않는다. 아래에는 신용정보법에 대해 고유하게 제기된 문제를 중심으로 주요 쟁점을 분석해보고자 한다.

가. 개인신용정보의 범위

개정된 개인정보 보호법과 신용정보법이 2020년 8월 5일 시행된 지 얼마 되지 않아, 법의 적용 범위를 둘러싼 갈등이 표출되었다. 2021년 2월 4일부터 금융위원회가 추진하고 있는 마이데이터 사업이 시행되는데, 전자상거래 업체들이 보유하고 있는 고객의 쇼핑 내역이 개인신용정보인지 여부를 둘러싸고 개인정보 보호위원회와 금융위원회의 이견이 표출된 것이다[160]. 전자상거래 업체 역시 자신들이 보유하고 있는 고객정보를 마이데이터 사업자에게 제공해야 하는 것에 반대했다.

논란이 마이데이터 사업을 둘러싸고 벌어지기는 했지만, 이는 근본적으로 개인신용정

160) 한국경제TV, 2020.8.13., "쇼핑내역은 개인정보 아닌 신용정보"...금융위, 행안부 패싱, <https://www.youtube.com/watch?v=efyadYn_VJs>.

보의 범위가 어디까지인지의 문제이다. 이는 곧 해당 개인정보에 개인정보 보호법을 적용할지, 혹은 신용정보법을 적용할지의 문제로 이어진다.

개인신용정보는 “기업 및 법인에 관한 정보를 제외한 살아 있는 개인에 관한 신용정보”이다(신용정보법 제2조 2호). 제2조 1호는 신용정보를 “금융거래 등 상거래에서 거래 상대방의 신용을 판단할 때 필요한 정보”로 정의하고 있는데, 1호 나목에 따라 ‘신용정보주체의 거래내용을 판단할 수 있는 정보’도 신용정보에 포함되도록 규정되어 있다. 그런데 문제는 A씨가 O월 O일 O시에 OO 쇼핑몰에서 OO색깔, OO사이즈, 모델명OO인 운동화를 샀다는 정보가 신용정보냐는 것이다[161]. 금융위원회는 제2조 제1호 나목에서 신용정보주체의 거래내용을 판단할 수 있는 정보도 신용정보로 규정하고 있고, 제2조 제1의3호 마목은 신용정보주체의 거래내용을 판단할 수 있는 정보로 “「상법」 제46조에 따른 상행위에 따른 상거래의 종류, 기간, 내용, 조건 등에 관한 정보”도 포함하고 있기 때문에 쇼핑몰 거래 내역도 개인신용정보라는 입장이다. 그러나 ‘신용정보주체의 거래내용을 판단할 수 있는 정보’를 무조건 신용정보라고 할 수 있는지에 대해서는 의문이 제기된다. 금융거래의 종류, 기간, 금액, 금리, 한도 등을 규정하고 있는 제2조 제1의3호 가목부터 라목의 경우는 변제능력에 해당되는 신용을 측정하는 정보가 될 수 있다고 볼 수 있으나, 마목에서 규정하고 있는 ‘「상법」 제46조에 따른 상행위에 따른 상거래의 종류, 기간, 내용, 조건 등에 관한 정보’의 경우는 변제능력이 기초가 되는 신용정보라기보다는 오히려 정보주체의 취향이나 성향정보라고 보는 것이 타당하기 때문이다. 「상법」 제46조 각 호에 규정된 상행위들은 인류가 정형적으로 수행해온 모든 상거래 행위를 열거해 놓은 것으로, 이를 신용정보법에서 규율할 경우 인류의 정형적 거래와 관련된 모든 정보가 신용정보법의 규율 하에 놓이게 된다. 이는 개인정보 보호법의 적용을 축소, 형해화하는 결과를 초래할 위험이 있다[162].

애초에 2020년 신용정보법 개정 이전에는 모든 상거래가 신용정보로 규정되지 않았다. 개정 전 신용정보법은 제2조 1호 나목에서 ’신용정보주체의 거래내용을 판단할 수 있는 정보’를 규정하고 그 구체적인 내용은 시행령에 위임하였으며, 시행령 제2조 2호는 신용

161) 뉴스1, 2020.10.23., '주문내역' 논란에 '삐걱' 마이데이터…입법조사처 "범위 명확하게", <https://www.news1.kr/articles/?4095446>.

162) 김현경(2020), 개인신용정보의 범위에 대한 비판적 고찰- 상행위 거래정보는 모두 개인신용정보인가?, 개인정보보호법학회 특별세미나(2020.10.12.) 발표문, pp.8-9.

정보주체의 거래내용을 판단할 수 있는 정보를 “대출, 보증, 담보제공, 당좌거래(가계당좌거래를 포함한다), 신용카드, 할부금융, 시설대여와 금융거래 등 상거래와 관련하여 그 거래의 종류, 기간, 금액 및 한도 등에 관한 사항”이라고 규정하고 있다. 즉, 현재와 같이 일반적인 상거래의 종류, 기간, 내용, 조건 등에 관한 정보가 아니라 금융거래와 관련된 상거래로 좁게 규정되어 있던 것이다. 2020년 신용정보법 개정을 통해 이처럼 ’신용정보주체의 거래내용을 판단할 수 있는 정보’를 확대한 것은 신용정보법의 적용 범위를 확대하기 위한 의도로 보여진다. 이는 개인정보에 대한 감독권한이 개인정보 보호위원회와 금융위원회로 이원화된 상황이 초래한 혼란과 갈등으로 볼 수 있다. 이러한 혼란을 해소하기 위해서는 신용정보법은 금융 및 신용정보 산업에 대한 규율을 다루고 개인정보와 관련된 규율은 개인정보 보호법으로 일원화할 필요가 있다.

나. 익명처리에 대한 적정성 평가

신용정보법은 개인정보 보호법과 달리 제2조 17호에서 ‘익명처리’를 “더 이상 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리하는 것”으로 정의하고 있다. 개인정보 보호법에는 ‘익명처리’라는 개념을 사용하고는 있지만 이를 정의하고 있지는 않다. 다만, 제58조의2에서 “시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보”에는 개인정보 보호법이 적용되지 않는다고 규정하고 있는데, 이처럼 더 이상 개인을 알아볼 수 없는 정보를 익명정보라고 할 수 있다. GDPR 역시 가명처리의 개념은 정의하고 있지만, 익명처리에 대한 정의는 규정하고 있지 않다.

신용정보법 제40조의2는 가명처리 및 익명처리에 대한 행위규칙을 규정하고 있는데, 신용정보회사등은 개인신용정보에 대한 익명처리가 적정하게 이루어졌는지 여부에 대하여 금융위원회에 그 심사를 요청할 수 있고(제3항), 금융위원회가 이를 심사하여 적정하게 익명처리가 이루어졌다고 인정한 경우, 더 이상 해당 개인인 신용정보주체를 알아볼 수 없는 정보로 추정(제4항)하도록 하고 있다. 금융위원회는 심사 및 인정 업무를 제26조의4에 따른 데이터전문기관에 위탁할 수 있다(제5항).

그런데 이와 유사한 규정이 2016년 <개인정보 비식별 조치 가이드라인>에도 포함되어

있었다. 가이드라인은 개인정보처리자가 개인정보를 비식별 조치한 경우 평가단을 통해 적정성 평가를 하도록 했고, 가이드라인에 따라 적정하게 비식별 조치가 된 정보는 더 이상 특정 개인을 알아볼 수가 없으므로 개인정보가 아닌 것으로 추정된다고 규정했다. 다만, 불특정 다수에게 공개하는 것은 식별 위험이 크므로 원칙적으로 금지하였다.

신용정보법상 익명처리 적정성 평가는 자체적인 평가단이 아니라 데이터전문기관을 통해 수행된다는 점, 그리고 익명처리가 된 것으로 추정하여 개인정보 보호법이나 신용정보법을 적용받지 않고 자유롭게 사용할 수 있도록 한다는 점에서, 기존 가이드라인의 적정성 평가와 차이가 있다. 그러나 여전히 문제는 적정성 평가가 제대로 되지 않았을 경우, 즉 익명처리가 된 것으로 생각했으나 제대로 익명처리가 되지 않아 정보주체에게 피해가 발생할 경우, 누가 책임을 질 것인가이다. 1차적으로는 당연히 제대로 익명처리를 하지 않은 개인정보처리자가 책임을 져야할 것이다. 그러나 적정성 평가를 잘못하여 피해를 야기한 금융위원회 및 데이터전문기관은 어떠한 책임을 지는 것인지 명확하지 않다. 아무런 책임도 없다면 산업 활성화를 명분으로 손쉽게 적정성 평가를 남발할 가능성을 배제할 수 없다[163].

다. 공개된 SNS 정보의 수집과 표현의 자유 침해 우려

20대 국회에서 김병욱 의원이 대표발의한 신용정보법 개정안은 제15조제2항에서 신용정보회사등이 개인신용정보를 수집하는 때에는 해당 신용정보주체의 동의를 받아야 하지만, 동의를 받지 않아도 되는 예외를 규정하면서 다목에 “신용정보주체가 스스로 사회관계망서비스 등에 직접 또는 제3자를 통하여 공개한 정보”를 포함하였다. 금융위원회가 2018년 11월 21일 발표한 보도자료에 따르면, 이는 “비금융 개인신용정보(통신・전기・가스 요금납부, 온라인 쇼핑 내역, SNS정보 등)만을 활용하여 개인신용을 평가”하는 비금융정보 전문 신용평가사(CB)를 도입하려는 의도와 연결되어 있다. 금융위원회는 이 정책의 목적을 “비금융정보를 활용한 대안적 신용평가결과를 활용하여 사회초년생, 주부 등 금융이력이 부족한 소비자의 금융접근성 제고”를 위함이라고 밝혔다[164].

163) 건강과대안 외(2018), 2018.12.12., “신용정보법 개정안(김병욱 의원 대표발의)에 대한 시민사회 의견서“, <http://www.privacy.or.kr/archives/5708>.
164) 금융위원회, 2018.11.21., “데이터 경제 활성화를 위한 신용정보산업 선진화 방안 -신용조회업에서 금융분야 핵심 데이터 산업으로-”,

그러나 시민사회단체들은 이는 정보주체의 개인정보 권리의 침해이자 표현의 자유를 위축시킬 수 있다고 반발하였다[165]. 공개된 개인정보 역시 개인정보이며 이는 국내 헌법재판소[166] 및 대법원[167]의 판결을 통해 인정된 것이므로, SNS를 통해 공개한 정보라도 정보주체의 동의 없이 수집할 수 있도록 하는 것은 개인정보 자기결정권의 제한이라는 것이다. 또한, SNS를 통해 공개된 정보를 신용평가 목적으로 활용한다면, 자신의 SNS 정보들이 혹여나 신용평가에 부정적으로 사용될 것을 우려하여 이용자들의 SNS 사용이 위축될 우려가 있다고 비판하였다. 오타가 많거나, 개인의 병명 등 민감한 내용을 포함하고 있거나, 정부 혹은 기업에 비판적인 내용이거나, 술자리 등 방탕한 면모를 보여주는 등의 SNS 정보 등 어떠한 내용이 신용평가에 활용될지 불명확하기 때문이다.

이러한 비판을 일부 수용하여 신용정보법 개정안은 국회 논의 과정에서 수정되었다. 현재 신용정보법 제15조 제2항 제2호 다목은 "신용정보주체가 스스로 사회관계망서비스 등에 직접 또는 제3자를 통하여 공개한 정보. 이 경우 대통령령으로 정하는 바에 따라 해당 신용정보주체의 동의가 있었다고 객관적으로 인정되는 범위 내로 한정한다"고 수정되었다. 신용정보법 시행령 제13조는 신용정보주체의 동의가 있었다고 객관적으로 인정되는 범위의 정보를 판단하기 위한 고려 요소로 다음과 같은 6가지를 제시하고 있다.

1. 공개된 개인정보의 성격, 공개의 형태, 대상 범위
2. 제1호로부터 추단되는 신용정보주체의 공개 의도 및 목적
3. 신용정보회사등의 개인정보 처리의 형태
4. 수집 목적이 신용정보주체의 원래의 공개 목적과 상당한 관련성이 있는지 여부
5. 정보 제공으로 인하여 공개의 대상 범위가 원래의 것과 달라졌는지 여부
6. 개인정보의 성질 및 가치와 이를 활용해야 할 사회 · 경제적 필요성

이는 대법원의 판결문 내용을 참조한 것이다. 그런데, '개인정보의 성질 및 가치와 이를 활용하여야 할 사회·경제적 필요성'은 판결문에서 언급하고 있는 표현이기는 하지만, '정보처리로 얻은 이익의 정도와 그 정보처리로 인하여 정보주체의 이익이 침해

<https://www.korea.kr/news/pressReleaseView.do?newsId=156304772>.

165) 건강과대안 외(2018), 2018.12.12., "신용정보법 개정안(김병욱 의원 대표발의)에 대한 시민사회 의견서", <http://www.privacy.or.kr/archives/5708>.

166) 헌법재판소 2005. 5. 26. 99헌마513, 2004헌마190(병합) 전원재판부 판결.

167) 대법원 2016. 8. 17. 선고, 2014다235080 판결.

될 우려의 정도’를 형량하여 위법성을 판단하는데 사용되는 기준으로 사용되었다. 만일 이 기준이 포함된다면 ‘정보주체의 이익이 침해될 우려의 정도’ 역시 포함되는 것이 적절할 것이다.

그러나 이처럼 공개된 개인정보의 동의 없는 활용의 조건을 기존 대법원의 판결문을 참조하여 규정했다고 하더라도 신용정보법에 해당 규정을 포함하는 문제는 여전히 논란의 여지가 있다. 왜냐하면 대법원이 일정한 경우 공개된 개인정보에 대해 별도의 동의를 받을 필요가 없다고 본 것은 “또다시 정보주체의 별도의 동의를 받을 것을 요구한다면 이는 정보주체의 공개의사에도 부합하지 아니하거니와 정보주체나 개인정보처리자에게 무의미한 동의절차를 밟기 위한 비용만을 부담시키는 결과”를 초래하기 때문인데, 과연 신용평가 목적으로 SNS 정보를 활용하는 것이 이에 해당할 수 있을지는 의문이다.

국가인권위원회 역시 신용정보법 시행령(안)에 대해 의견을 표명하면서, “정보 주체가 SNS에 스스로 공개한 개인정보라고 하더라도 신용정보 회사가 아무런 제약 없이 수집·이용할 수 있다고 보기는 어렵다”며 “정보 주체가 신용평가회사로 하여금 자신의 SNS 정보를 수집해 신용평가에 활용하도록 하겠다는 ‘의도와 목적’을 가지고 정보를 공개하는 경우는 현실적으로 기대하기 어렵”기 때문에 “결과적으로 신용정보회사의 임의적 판단에 따른 과도한 SNS 정보 수집이 우려된다”고 지적했다. 또한, 인권위는 “정보 주체의 요구가 있을 경우 정보 수집 출처와 처리 목적, 정보 삭제나 처리 정지 권리 등을 알리도록 하는 규정을 추가할 필요가 있다”고 권고했다[168].

라. 개인신용정보 전송요구권과 마이데이터 사업

2018년 11월, 금융위원회가 발표한 <데이터 경제 활성화를 위한 신용정보산업 선진화 방안>의 배경 중 하나는 “데이터 경제 활성화를 위해 금융분야 데이터 혁신을 가속화하고 데이터 산업을 육성”하는 것이며, 이를 위한 여러 과제를 제안하고 있는데 그 중 하나가 마이데이터 산업의 도입이다. 마이데이터 사업(본인신용정보관리업)은 “금융권 및 공공기관 등에 흩어진 개인의 신용정보를 통합하여 일괄조회·관리·활용할 수 있도록” 지원하는 사업으로 개인의 정보관리를 도울 뿐만 아니라, 맞춤형 상품추천이나 금

168) 연합뉴스, 2020.6.8., “인권위, 데이터3법 정부 시행령안 "과도한 정보수집 우려" 표명”, <https://www.yna.co.kr/view/AKR20200607030800004>.

융상품 자문 등 추가적인 서비스 개발이 가능할 것으로 전망하고 있다.

정보주체의 동의에 기반한 개인정보의 통합 관리는 기존의 법제 하에서도 가능한데, 개정 신용정보법은 '개인신용정보 전송요구권'을 신설하여 마이데이터 사업자가 보다 효율적으로 개인정보를 수집할 수 있는 수단을 제공하고 있다. 2021년 2월 4일 시행 예정인 제33조의2조는 개인인 신용정보주체가 신용정보제공·이용자등에 대하여 그가 보유하고 있는 자신에 관한 개인신용정보를 본인 혹은 본인신용정보관리회사 등에게 전송하여 줄 것을 요구할 수 있도록 하고 있다. 다만, 신용정보제공·이용자등이 개인신용정보를 기초로 별도로 생성하거나 가공한 신용정보는 제외된다(제33조의2조제2항제3호). 또한 '컴퓨터 등 정보처리장치로 처리가 가능한 형태'로 전송할 것을 요구하고 있다.

금융위원회는 전송요구권이 GDPR 제20조 개인정보 이동권을 국내에 도입한 것이라고 한다. GDPR 제20조는 "개인정보주체는 컨트롤러에게 제공한 본인에 관련된 개인정보를 체계적이고, 통상적으로 사용되며 기계 판독이 가능한 형식으로 수령할 권리가 있으며, 개인정보를 제공 받은 컨트롤러로부터 방해받지 않고 다른 컨트롤러에게 해당 개인정보를 이전할 권리를 가진다"고 규정하고 있다.

그러나 GDPR의 개인정보 이동권이 예정하고 있는 모델은 마이데이터 사업 모델과 다르다[169]. 마이데이터 사업은 서로 다른 사업자들이 보유하고 있는 개인정보의 통합을 지향하는 반면, GDPR의 개인정보 이동권은 이용자가 한 서비스 제공자로부터 다른 서비스 제공자로 전환하는 모델을 상정하고 있는 것으로 보인다. 29조 작업반의 개인정보 이동권 가이드라인[170]은 동 권리의 의의로 이용자가 서비스 제공자를 쉽게 전환할 수 있도록 하여 서비스 제공자 사이의 경쟁을 촉진하고, 디지털 단일시장 전략의 맥락에서 새로운 서비스의 형성을 가능하게 하며, 개인정보에 대한 개인의 권리 및 통제의 보장을 통해 정보주체와 처리자 사이의 관계의 재균형(re-balance)의 기회를 제공함을 들고 있다. 금융위원회는 명목상으로는 "신용정보에 대한 통제권을 정보주체인 개인에게 되돌려주는" 것[171]을 내세우고 있지만, 신용정보산업 선진화 방안의 전반적인 맥락을 고려하면

169) Robert Madge(2017), GDPR: data portability is a false promise.
170) ARTICLE 29 DATA PROTECTION WORKING PARTY(2017a), Guidelines on the right to data portability, 16/EN WP 242 rev.01, Adopted on 13 December 2016, As last Revised and adopted on 5 April 2017.
171) 금융위원회, 2018.11.21., "데이터 경제 활성화를 위한 신용정보산업 선진화 방안 -신용조회업에서 금융분야 핵심 데이터 산업으로-",

그 이면에는 개인정보의 활용을 촉진하겠다는 의도가 깔려있다. 제33조의2 제4항에서 ‘정기적으로 같은 내역의 개인신용정보를 전송하여 줄 것을 요구할 수’ 있도록 한 것도 GDPR에는 없는 내용인데, 이 역시 마이데이터 사업자의 편의를 고려한 부분이다. 그러나 정보주체가 동의를 할 때 서비스에 대한 설명을 제대로 제공받지 못하거나, 혹은 서비스에 대한 충분한 이해 없이 동의를 하는 경우가 많은 현실을 고려할 때, 마이데이터 사업이 정보주체의 충분한 인지 없는 개인정보의 통합이나 유통을 야기할 수 있다는 우려가 제기될 수 있다. 향후 마이데이터 사업이 시행되면 정보주체의 인지 정도나 권리 보장 실태에 대한 점검이 필요하다.

개인정보 이동권이 충분한 논의를 거쳐 개인정보 보호법에 신설된 것이 아니라, 신용정보법에 애매한 형태로 먼저 신설된 것도 문제다. GDPR의 개인정보 이동권은 모든 개인정보처리자를 대상으로 한 반면, 신용정보법상의 전송요구권은 그 대상이 한정적이면서도 신용정보법의 주 규율대상인 금융기관을 넘어 공공기관 및 일반 전자상거래업체까지 확대하고 있다. 이렇게 될 경우 마이데이터가 개인신용정보가 아니라 일반 개인정보 영역에도 도입되는 효과를 낳으면서도 신용정보법의 규율을 받게 되는 문제가 발생하는 것이다[172].

마. 법체계 문제 - 하위 규범으로의 지나친 위임

신용정보법이 지나치게 많은 내용들을 하위 법령에 위임하고 있는 점도 문제로 지적된다. 또한 법률에서 시행령에 위임한 사항을 더 구체화하지 않고 고시로 재위임하고 있는 조항도 다수 발견된다. 신용정보법에서 대통령령으로 위임하고 있는 사항이 무려 약 250여 개에 이른다고 한다. 특히 ‘신용정보’의 개념과 관련하여 무려 17부분을 대통령령에 위임하였다[173].

예를 들어 신용정보법 제2조 제1의2는 “제1호 가목의 ‘특정 신용정보주체를 식별할 수 있는 정보’란 다음 각 목의 정보를 말한다”라면서 제1의2의 가목에서 “살아 있는 개인에 관한 정보로서 다음 각각의 정보”를, 그 아래에 “1) 성명, 주소, 전화번호 및

<https://www.korea.kr/news/pressReleaseView.do?newsId=156304772>.
172) 김현경(2020), 앞의 글, p13.
173) 김현경(2020), 위의 글, p21.

그 밖에 이와 유사한 정보로서 대통령령으로 정하는 정보”를 규정하면서, 시행령에 다시 위임하고 있다. 시행령 제2조 1항은 제2조 제1호의2 가목1)의 “대통령령으로 정하는 정보”로 1. 전자우편주소 2. 사회 관계망 서비스(Social Network Service) 주소 3. 그 밖에 제1호 및 제2호의 정보와 유사한 정보로서 금융위원회가 정하여 고시하는 정보로 규정하면서 다시 금융위원회의 고시로 위임하고 있다. 고시인 <신용정보업 감독규정> 제2조의2는 이에 해당하는 정보로서, 1. 성별, 국적, 그 밖에 이와 유사한 정보 2. 「민법」에 따른 거소를 규정하고 있다. 이런 식으로 사실상 법에서 규정한 것과 별다른 차이가 없는 정보에 대해 시행령과 고시로 위임하는 구조를 갖추고 있다. 이러한 방식의 과도한 위임은 행정기관에 입법권을 부여하는 것이나 다름없다.

<표3-3> 하위 규범으로의 과도한 위임 사례

신용정보법	시행령	고시 (신용정보업감독규정)
제2조 1의2. 제1호가목의 “특정 신용정보주체를 식별할 수 있는 정보“란 다음 각 목의 정보를 말한다. 가. 살아 있는 개인에 관한 정보로서 다음 각각의 정보 1) 성명, 주소, 전화번호 및 그 밖에 이와 유사한 정보로서 대통령령으로 정하는 정보	제2조(정의) ① 「신용정보의 이용 및 보호에 관한 법률」(이하 “법“이라 한다) 제2조제1호의2가목1)에서 “대통령령으로 정하는 정보“란 다음 각 호의 정보를 말한다. 1. 전자우편주소 2. 사회 관계망 서비스(Social Network Service) 주소 3. 그 밖에 제1호 및 제2호의 정보와 유사한 정보로서 금융위원회가 정하여 고시하는 정보	제2조의2(신용정보의 범위) ① 영 제2조제1항제3호에서 “금융위원회가 정하여 고시하는 정보“란 다음 각 호의 정보를 말한다. 1. 성별, 국적, 그 밖에 이와 유사한 정보 2. 「민법」에 따른 거소

입법자의 의사와 배치되는 것으로 추정되는 재위임 사례도 나타난다[174]. 아래 표에서 볼 수 있는 바와 같이, 법률 제2조 제9호의2 가~라목에 비추어 보아 시행령 제2조 제23항 제1호에서 정한 “법 제1호의3 가목3) 및 같은 호 같은 목 4)”을 본인신용정보관리업의 영업 대상에 포함하고자 했다면, 법률에서 이를 규정했을 것이다.

174) 경실련 외, 2020.5.11., “개인정보보호법 및 신용정보보호법 시행령(안)에 대한 시민사회 의견서”, <https://act.jinbo.net/wp/42829/>.

<표3-4> 입법자의 의사와 배치될 수 있는 시행령 위임 사례

신용정보법	신용정보법 시행령
9의2. “본인신용정보관리업“이란 개인인 신용정보주체의 신용관리를 지원하기 위하여 다음 각 목의 전부 또는 일부의 신용정보를 대통령령으로 정하는 방식으로 통합하여 그 신용정보주체에게 제공하는 행위를 영업으로 하는 것을 말한다. 가. 제1호의3가목1)ㆍ2) 및 나목의 신용정보로서 대통령령으로 정하는 정보 나. 제1호의3다목의 신용정보로서 대통령령으로 정하는 정보 다. 제1호의3라목의 신용정보로서 대통령령으로 정하는 정보 라. 제1호의3마목의 신용정보로서 대통령령으로 정하는 정보 마. 그 밖에 신용정보주체 본인의 신용관리를 위하여 필요한 정보로서 대통령령으로 정하는 정보	제2조(정의) ㉓ 법 제2조제9호의2마목에서 “대통령령으로 정하는 정보“란 다음 각 호의 정보를 말한다. 1. 법 제2조제1호의3가목3) 및 4)의 신용정보로서 별표 1에 해당하는 정보 2. 그 밖에 금융위원회가 정하여 고시하는 정보

그럼에도 불구하고 이를 법률에 포함하지 않은 것(즉, 법률 제2조 제9호의 2에서 가목 1),2) 및 나목만을 포함하고 있을 뿐 가목3)과 4)는 제외하고 있음)은 입법자의 의사라고 이해하는 것이 타당하다. 금융위원회가 이를 시행령에 포함한 것은 입법자의 의사와 배치될 수 있다.

제3절 국내 개인정보 보호법제 개선 방향

지금까지 소위 데이터 3법을 둘러싼 주요 쟁점을 살펴보았다. 많은 논란에도 불구하고 결국 2020년 1월 9일 데이터 3법은 국회를 통과하였고 8월 5일부터 시행되었다. 개인정보 보호법 시행에 맞춰 통합 개인정보 보호위원회도 출범하였다. 통합 개인정보 보호위원회는 당분간 조직의 정비, 가이드라인 및 해설서 등의 제·개정, 결합전문기관 지정 등 데이터 3법 이행에 집중하겠지만, 멀지 않은 시점에 개인정보 보호법의 개정도 불가피할

것으로 보인다. 정보통신망법의 개인정보 관련 조항이 특례 형태로 임시적으로 개인정보 보호법에 통합되었기 때문에 관련 조항들을 재정비하는 작업이 불가피할 뿐만 아니라, 빅데이터, 인공지능 등 산업의 발전에 조응한 개인정보 보호법의 업그레이드 역시 필요하기 때문이다.

나아가 유럽연합으로부터 GDPR 적정성 결정을 받기 위해서라도 국내 개인정보 보호 법제를 국제적인 규범에 맞게 개선할 필요가 있다. 전술한 바와 같이 GDPR 적정성 결정 체결을 위한 기준을 충족하기 위해 행정안전부 뿐만 아니라 방송통신위원회의 개인정보 감독권한까지 개인정보 보호법 개정을 통해 통합 개인정보 보호위원회로 이관하였다. 이에 통합 개인정보 보호위원회는 2020년 8월 5일 새롭게 발족한 이후 유럽연합과의 적정성 협상을 주도하고 있다. 적정성 결정의 가장 큰 걸림돌이 독립적인 감독기관의 존재였기 때문에, 개인정보 보호위원회는 무난하게 적정성 결정을 받을 수 있을 것으로 전망하고 있다. 그러나 코로나19로 인한 여파도 있겠지만, 2020년 내에 적정성 결정을 체결할 수 있을지는 불투명하다. 또한 유럽연합과 미국과의 프라이버시 쉴드 협정을 무효화한, 2020년 7월 유럽사법재판소의 판결을 고려하면, 정보수사기관의 개인정보 접근에 대해 더욱 엄격하게 판단할 가능성이 높기 때문에 한국의 개인정보 제도와 관행이 적정성 결정을 받을 수 있을지 낙관하기 힘들다[175]. 물론 유럽연합이 일본과 상호 적정성 결정을 합의한 것을 보면, 적정성 결정에 정치적인 고려가 영향을 미치고 있음을 알 수 있다. 다만 일본의 경우 적정성 결정을 위해 유럽으로부터 이전된 개인정보에만 적용되는 추가 규칙을 제정하였는데, GDPR에 대한 2년 평가에서 EDPB가 이러한 방식의 적정성 결정에 대해 유보적인 평가를 내린 것을 고려하면, 한국 역시 현재의 법제가 GDPR에 견주어 미흡하기 때문에 이를 보완할만한 추가 규칙을 만들어야 하는 상황이 긍정적으로 작용하기 힘들다. 설사 이번에 적정성 결정을 받는다고 하더라도, GDPR 적정성 결정은 정기적으로 재평가를 한다는 점을 고려하면 GDPR과 실질적으로 동등한 수준으로 국내 개인정보 보호 법제를 개선하는 것이 근본적인 해결책이 될 것이다.

지금까지의 분석을 토대로 국내 개인정보 보호 법제의 개선 방향을 제시하자면 다음

175) 세계일보, 윤종인 개인정보보호위원회 위원장, 2020.10.27., “온라인상 ‘잊힐 권리’ EU선 명문화… 국내도 법제화 검토”, <http://m.segye.com/view/20201027521861>.

과 같다.

첫째, 우선 개인정보 보호 법제에 여전히 남아있는 모호함을 해소하는 방향으로의 정비가 필요하다. 이미 언급하였듯이, 정보통신망법의 개인정보 관련 조항이 개인정보 보호법의 관련 조항에 융합되지 못하고, 특례 형식으로 임시적으로만 합쳐진 상황이다. 따라서 정보통신서비스 제공자에게만 적용되어야 할 내용이 아니라면 하루빨리 관련 조항을 적절하게 통일하는 것이 수범자의 혼란을 최소화하는 길이다.

또한 개정 개인정보 보호법이 국회에서 충분한 논의를 거치지 못한 탓인지, 개념상 모호한 규정도 존재한다. 예를 들어, 이번 개정의 핵심 내용 중의 하나인 제28조의2에서는 “개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다”고 규정하고 있는데, ‘가명정보’를 처리할 수 있다고 표현하고 있지만 실제 의미하는 바는 ‘가명처리’로 보여진다. 즉, 이미 가명처리된 정보를 통계작성 목적 등으로 처리하는 것이 아니라, 개인정보를 통계작성 목적 등으로 가명처리할 수 있도록 하겠다는 것이 입법자의 의도일 것이다. 이러한 모호함이 해소되지 않는다면, 제28조의7의 경우에도 (이 조항 자체의 문제점과 별개로) 가명정보 뿐만 아니라 가명처리에도 이 조항이 적용되는 것으로 잘못 해석될 수 있다.

앞서 분석한 바와 같이 의료정보를 비롯한 민감정보에도 제3절 가명정보의 처리에 관한 특례가 적용되는지도 명확하지 않다. 정부는 적용된다고 해석을 하면서 밀어붙이고 있지만, 가장 바람직한 것은 법에서 명확하게 규정하는 것이다. 이를 위해서는 제23조 민감정보에 대한 규정을 현실에 맞게 민감정보의 처리가 가능한 경우를 보다 구체적으로 반영할 필요가 있다.

둘째, 개인정보 보호법과 신용정보법, 그리고 위치정보법 등 개인정보 보호 법제를 일원화하는 방향으로 추가 정비할 필요가 있다. 데이터 3법의 개정 목적 중의 하나가 개인정보 보호 법제 및 감독체계의 일원화였음에도 불구하고, 그러한 목표를 달성하는데 한계가 있었음은 앞서 본 바와 같다. 이 때문에 소비자의 쇼핑몰 이용내역도 마이데이터 사업자에게 이전해야 하는지, 즉 개인신용정보의 범위를 둘러싼 부처간, 사업자간 갈등이 노정되기도 했다. 이러한 문제를 근본적으로 해소하기 위해서는 신용정보법의 개인정보 관련 조항을 개인정보 보호법으로 일원화하고, 금융위원회의 개인정보 감독권한도 개인정보 보호위원회로 이관하는 방향으로 법제 개선이 이루어져야 한다. 또한 지난 데이

터 3법 처리 과정에서는 제외되었던 위치정보의 보호 및 이용 등에 관한 법률(위치정보법)의 개인정보 보호법으로의 통합 역시 검토되어야 할 것이다.

셋째, 빅데이터, 인공지능 등 신기술 환경에서 정보주체의 권리를 보호하고 개인정보처리자의 책임성을 강화하기 위한 새로운 규범들을 도입할 필요가 있다. 데이터 3법의 경우 빅데이터 산업발전을 명분으로 개정이 되었지만, 사실상 가명정보 개념 및 결합전문기관 도입을 통한, 정보주체의 동의 없는 개인정보의 활용에 방점이 있었다. 개인정보의 안전한 활용을 명분으로 통합 개인정보 보호위원회가 신설되기는 했지만, 이는 신기술 환경에 관련된 쟁점이라기보다는, 2000년대 중반에 발의된 개인정보 보호법 제정안에 이미 포함되었었던 내용이다. GDPR의 경우 신기술 환경에서 정보주체의 권리를 보호하기 위해 기존에 개인정보보호 디렉티브에 있던 권리도 확대·강화하는 한편, 개인정보 이동권을 새롭게 도입하였다. 특히 개인에 대한 프로파일링과 개인에 큰 영향을 미치는 자동화된 처리가 보편화되어 가는 상황에서 '프로파일링 등 자동화된 개별 의사결정에 대한 정보주체의 권리' 도입은 매우 시급하다.

GDPR에서 개인정보 보호 규범을 준수할 컨트롤러의 책임과 입증의 의무를 부과하고 컨트롤러의 책임성을 강화하기 위한 다양한 조치를 도입한 것을 참조하여, 국내 개인정보 보호법에서도 개인정보처리자의 책임성 강화를 위한 조항을 도입할 필요가 있다. 현재 개인정보 보호책임자가 개인정보 집행의 책임을 맡는 위치라면, 개인정보처리자를 자문하고 감독하는 지위를 가진, 독립적인 정보보호 책임자(DPO) 제도를 국내에서도 도입할 만하다. 공공기관의 일부 개인정보 파일에만 적용되는 개인정보 영향평가를 실질화하고, 개인정보 침해 위험이 큰 민간의 개인정보 처리로 확대할 필요가 있다. 설계 및 기본설정에 의한 개인정보 보호 등의 제도 도입도 검토가 필요하다.

또한 국제적인 정보유통이 보편화되는 상황을 고려하여, 우리 국민들의 개인정보가 국외로 이전되더라도 안전하게 처리될 수 있도록 다른 나라에 대한 적정성 결정 등 다양한 방법을 제시할 필요가 있다.

넷째, 지난 2014년 에드워드 스노든이 미국 국가안보국(NSA)의 인터넷 대량 감청을 폭로한 이후 유럽연합의 적정성 평가 기준으로 각국의 정보수사기관의 개인정보 접근 문제의 중요성이 커지고 있고 2020년에 유럽연합과 미국 사이의 프라이버시 쉴드 협정도 유럽사법재판소에 의해 무효가 되었다는 점을 고려하면, 한국 역시 정보수사기관의 개인정

보 처리 원칙과 관행 문제를 재검토할 수밖에 없다. 국내 개인정보 보호법의 경우 정보 수사기관의 개인정보 처리에 대해서는 폭넓은 예외를 허용하고 있는 만큼, 국제적인 기준에 맞게 규범을 재정비하고 이들 기관에 대한 감독을 강화할 수 있는 방안을 모색해야 한다.

제4장 정보주체의 권리보호

제1절 정보주체의 권리보호를 위한 개인정보 처리원칙

1. GDPR의 개인정보 처리원칙

GDPR은 개인정보 처리를 적법성·공정성·투명성 원칙(lawfulness, fairness and transparency)에 의해야 할 것을 선언하고 규정한다. 개인정보는 정보주체에 대해 적법하고, 공정하며, 투명하게 처리되어야 한다(제5조 제1항 (a)호). 개인정보 처리는 적법해야 하며 적법성을 인정받기 위해서는 처리를 위한 구체적인 근거를 제시해야 한다. GDPR은 개인정보 처리의 합법적 근거를 제6조(처리의 적법성), 제7조(동의의 조건), 제9조(민감정보의 처리), 제10조(범죄정보의 처리)에서 상세히 규정하고 있다. 이러한 적법한 근거를 개인정보 처리와 관련해서 제시하지 못하면 처리는 불법적인 것이 되어 적법성 원칙을 위반하게 된다. 또한 적법성은 넓은 의미에서 인권법, 민・형법을 비롯한 각종 법령이나 계약상의 의무를 위반하지 않아야 한다는 것을 의미한다.

개인정보 처리의 공정성 원칙에 따라 모든 사람이 합리적으로 기대할 수 있는 방법으로 개인정보를 처리하고, 정보주체에게 부당한 영향을 미치는 방법으로 개인정보를 이용하지 않아야 한다. 수집・이용 방법이 다른 사람들에게 공정하더라도 특정 개인에게 불공평하다면 공정성 원칙 위반이 될 수 있다.

개인정보 처리의 투명성 원칙에 따라 개인정보를 누가, 어떤 목적으로, 어떤 정보를, 어떤 방식으로 처리하는지를 정보주체에게 명확하게 알려주어야 한다. 개인정보의 처리에 대해 정보주체에게 간결하고, 투명하며 이해하기 쉽고, 접근하기 쉬운 방식으로 정보를 제공해야 하며, 처리원칙을 위반하여 정보주체에게 불이익을 초래해서는 안 된다. 정보주체가 개인정보 처리 사실을 모르면 권리행사를 할 수 없기 때문에, 투명성 원칙은 정보주체로부터 개인정보를 직접 수집할 때도 중요하지만 정보주체 이외로부터 수집할 때 더 중요하다[176]. 이에 따라 GDPR은 제12조(정보주체의 권리 행사를 위한 투명한 정보, 통지 및 형식), 제13조 및 제14조(정보를 제공받을 권리), 제15조(정보주체의 접근권)

176) 한국인터넷진흥원(2020), pp46-47.

에서 투명성 원칙을 실현하기 위한 구체적인 방법을 규정하고 있다.

개인정보 처리는 목적 제한의 원칙(purpose limitation)에 따라야 한다. 개인정보는 구체적이고 명시적이며 적법한 목적을 위해 수집되어야 하고, 해당 목적과 양립하지 않는 방식으로 추가 처리되어서는 안 된다(제5조 제1항 (b)호). 본래의 개인정보를 수집하는 목적 외에 다른 목적으로 활용할 경우, 별도로 정보주체의 개별적인 동의를 획득하는 등의 추가 조치를 해야만 한다.

개인정보 처리는 데이터 최소화 원칙(data minimisation)에 따라야 한다. 개인정보는 처리되는 목적과 관련하여 적절하고 관련성이 있어야 하며, 이에 따라 필요한 범위로 제한되어야 한다(제5조 제1항 (c)호). 개인정보 수집 및 보유 사유를 명확히 입증할 수 있거나 집합(aggregated) 정보 또는 익명처리(anonymised)된 정보를 사용하여 적절한 보호조치를 보장해야 한다.

개인정보 처리는 정확성 원칙(accuracy)에 따라야 한다. 개인정보는 정확해야 하며 필요한 경우 최신 상태로 유지되어야 한다. 처리 목적과 관련하여 부정확한 개인정보는 지체 없이 삭제 또는 정정되도록 모든 적절한 조치가 시행되어야 한다(제5조 제1항 (d)호).

개인정보 처리는 보관기간 제한 원칙(storage limitation)에 따라야 한다. 개인정보는 처리 목적에 필요한 기간 내에서만 정보주체를 식별할 수 있는 형태로 보관되어야 한다(제5조 제1항 (e)호). 개인정보를 장기간 유지하는 경우, 유출 등에 의한 위험을 초래할 가능성이 크므로 처리 목적에 필요한 단기간의 보관기간을 설정하고 준수해야 한다.

개인정보 처리는 무결성과 기밀성 원칙(integrity and confidentiality)에 따라야 한다. 개인정보는 적절한 기술적, 조직적 조치를 활용해 무단 또는 불법 처리와 우발적 손실, 파괴, 손상을 막는 등 개인정보의 적절한 보안을 보장하는 방식으로 처리되어야 한다(제5조 제1항 (f)호).

컨트롤러는 개인정보 처리원칙을 엄격히 준수해야 할 책임(accountability)이 있다. 컨트롤러는 개인정보 처리원칙이 준수되도록 할 책임이 있으며, 이를 입증할 수도 있어야 한다(제5조 제2항).

2. 우리나라의 개인정보 보호 원칙

개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집할 것, 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하며 그 목적 외의 용도로 활용하지 말 것, 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 할 것, 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리할 것, 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하며 열람청구권 등 정보주체의 권리를 보장할 것, 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리할 것, 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 할 것, 개인정보 보호법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력할 것을 원칙으로 한다(개인정보 보호법 제3조).

3. 개선방안

우리나라의 개인정보 보호법상 개인정보 보호 원칙은 국제규범인 GDPR의 적법성·공정성·투명성 원칙에 입각하고 있다고 볼 수 있다. 하지만 개인정보 보호를 위한 가장 필요하고 중요한 원칙 규정의 경우에도, GDPR의 원칙 규정과 같이 보다 더 구체적으로 규정할 필요가 있다. 특히 개인정보 처리의 목적 제한의 원칙, 데이터 최소화 원칙, 정확성 원칙, 보관기간 제한 원칙, 무결성(완전성)과 기밀성 원칙에 대한 보다 자세한 내용을 규정하고, 적절한 기술적, 조직적 조치를 활용한 무단 또는 불법 처리 등으로부터 개인정보의 적절한 보안을 보장하는 방식으로 개인정보처리자가 처리할 것 등 보호조치 강화와 그 책임이 강조되어야 한다. 또한 개인정보 수집 및 보유 사유 등에 대한 명확한 증명책임, 개인정보 처리원칙의 준수책임과 그에 대한 증명책임을 개인정보처리자 등(개인정보의 처리 등에 대한 규범 준수자)에게 지우는 원칙이 필요하다.

제2절 정보주체의 개인정보 처리 정보를 제공받을 권리, 접근권, 수정권, 삭제권, 처리 제한권

1. GDPR의 정보주체의 권리

가. 개인정보 처리 정보를 제공받을 권리

GDPR은 정보주체가 개인정보 처리에 대해 자신의 권리를 쉽고 분명하게 행사할 수 있도록 하기 위해 컨트롤러가 개인정보에 대한 처리 정보를 정보주체에게 투명하게 통지하도록 하고 있다. 이를 위해 컨트롤러는 개인정보 처리와 관련하여 개인정보가 정보주체로부터 수집되는 경우 제공되어야 할 정보 및 정보주체로부터 수집되지 않는 경우 제공되어야 할 정보에서 명시된 일체의 정보와 정보주체의 각각 권리들에서 규정된 통지를 정확하고, 투명하며, 이해하기 쉬운 형식으로 명확하고 평이한 언어를 사용하여 정보주체에게 제공하기 위한 적절한 조치를 취해야 한다(제12조 제1항). 특히 아동을 특정 대상으로 할 때 더욱 적절한 조치를 하도록 해야 한다. 그리고 해당 정보는 서면이나 적절한 경우, 전자수단 등 기타 수단을 이용하여 제공되어야 하고 정보주체가 요청하는 경우, 다른 수단을 통해 정보주체의 신원이 입증되면, 해당 정보는 구두로 제공될 수 있도록 하고 있다.

컨트롤러는 해당 정보 및 통지를 효율적이고 간결하게 제시하여야 하는데, 예를 들어 온라인에서는 단계별 개인정보처리방침을 통해 정보주체가 특정 이슈를 찾기 위해서 많은 양의 텍스트를 전부 스크롤 할 필요 없이, 즉시 접근하고자 하는 개인정보처리방침의 특정 세션으로 이동하는 것과 같은 간결하고 투명한 방식을 채택할 수 있어야 한다. 또한 정보주체가 쉽게 이해할 수 있도록 하기 위해 컨트롤러는 해당 정보주체를 파악하고 평범한 구성원의 이해 수준을 확인할 필요가 있으며, 각 정보주체의 이해 수준이 다를 수 있기 때문에 컨트롤러는 정보·통지가 실제 이용자, 특히 아동의 경우에도 그에 맞추어져 있는지를 정기적으로 확인하고 조정하여야 한다. 정보주체가 정보를 찾아다닐 필요 없이 해당 정보를 어디서 접근할 수 있는지 바로 알 수 있도록 쉽게 접근할 수 있게 해야 한다. 이러한 경우로는 정보를 직접 제공하거나, 링크를 제공하거나, 분명한 안내 표

시를 하거나, 사람이 읽을 수 있는 자연어 질문의 답변 방식을 제공하여야 한다. 웹사이트를 유지하는 조직은 웹사이트에 개인정보 보호정책 및 고지를 게시할 수 있고, 그 링크는 웹사이트의 각 페이지에서 일반적으로 사용되는 용어 아래에 분명하게 눈에 띄는 방식으로 배치되어야 한다. 앱의 경우에는 다운로드 전에 온라인 스토어에서 필요한 정보를 이용할 수 있어야 하고, 앱을 설치한 후에는 정보 확인에 필요한 탭의 수가 2회를 넘어서는 안 되며, 앱에서 사용되는 메뉴 기능에 개인정보・정보보호 옵션이 포함되어야 한다. 온라인 맥락에서 개인정보의 수집 시점에 개인정보처리방침에 대한 링크를 제공하거나 개인정보를 수집하는 위치와 동일한 페이지에 해당 정보를 제공할 것이 권고된다[177].

컨트롤러는 하나 이상의 다른 언어를 사용하는 정보주체가 그 대상이 되는 경우, 각 해당 언어로 된 번역을 제공하여야 한다. 특히 아동을 대상으로 한 정보처리의 경우 모든 통지 및 의사표시는 해당 아동이 쉽게 이해할 수 있도록 아동에게 어울리고 공감이 가는 어휘, 어조, 문체를 사용함으로써 정보를 수신하는 아동이 메시지 및 정보가 자신을 대상으로 한 것임을 알 수 있도록 해야 한다. 또한 컨트롤러는 제공되는 상품 및 서비스가 장애인이나 정보에 접근하기 어려운 취약 계층 등에 의해 사용된다는 점을 인지하는 경우, 해당 정보주체와 관련된 투명성 의무를 준수하는 방법을 평가할 때 그들의 취약성을 고려하여야 한다[178].

컨트롤러는 정보주체의 권리행사를 용이하게 할 수 있도록 하여야 하고, 컨트롤러는 자신이 정보주체를 식별할 위치에 있지 아니하다는 점을 증명하지 않는 한, 정보주체가 자신의 각각 권리들을 행사하기 위한 요청을 거절해서는 안 된다(제12조 제2항). 컨트롤러는 정보주체가 자신의 각각 권리들을 행사하기 위한 요청에 대하여, 원칙적으로 요청을 접수한 후 1개월 이내 부당한 지체 없이 개인정보의 처리에 대한 일체의 정보 등을 제공해야 한다(제12조 제3항). 요청의 복잡성과 요청 횟수를 고려하여 필요한 경우 2개월 추가 연장하여 제공할 수 있으며, 다만 요청을 접수한 지 한 달 이내에 지체 사유와 이러한 연장에 대하여 고지하여야 한다. 요청에 대하여 조치를 취하지 않으면, 컨트롤러는 늦어도 접수 후 1개월 이내에 미조치 사유, 감독기구에 민원을 제기할 권리, 사법적 구

177) 한국인터넷진흥원(2020), 위의 글, pp129-130.
178) 한국인터넷진흥원(2020), 위의 글, p130.

제를 청구할 권리를 정보주체에게 고지하여야 한다(제12조 제4항).

이러한 정보주체의 개인정보 처리 정보에 대한 일체의 통지와 조치는 무상으로 제공하는 것을 원칙으로 한다(제12조 제5항). 다만, 정보주체의 요청이 명백하게 근거가 없거나 과도한 경우, 특히 요청이 반복될 경우, 컨트롤러는 관련 정보 또는 통지를 제공하거나 요청한 조치를 취하는 것에 소요되는 행정적 비용을 참작하여 합리적인 비용을 부과할 수 있거나, 해당 요청에 대한 응대를 거부할 수 있다(제12조 제5항 (a)호 및 (b)호). 이 때 컨트롤러는 해당 요청이 명백하게 근거가 없거나 과도하다는 사실을 증명할 책임이 있다.

정보주체에게 제공되는 정보는 예정된 처리에 대해 유의미한 개요를 제공하고자 표준화된 아이콘과 결합하여 가시적이고 이해하기 쉬우며 가독성이 뛰어난 방식으로 제공될 수 있으며, 해당 아이콘이 전자 방식으로 제공되는 경우에는 기계 판독이 가능해야 한다(제12조 제7항). 아이콘은 아주 많은 양의 서면 정보를 정보주체에게 제시하는 번잡함을 줄이고 투명성을 높이기 위하여 제안된 것이므로, 아이콘의 사용은 정보의 제공과 함께 이루어져야 하고 정보주체의 권리행사에 필요한 정보를 대체해서는 안 된다. 또한 컨트롤러의 의무준수에 대한 대체물로 사용되어서도 안 된다. 아이콘이 전자적으로 제공되는 경우 컴퓨터에 의한 판독이 가능(machine-readable)하여야 한다. 컴퓨터에 의한 판독이 가능한 형식은 개방 또는 독점적 형식, 공식 표준 또는 비공식일 수도 있다. 정보를 추출할 수 없거나 쉽게 추출할 수 없기에 자동처리가 제한되는 파일 형식으로 인코딩된 문서는 컴퓨터에 의한 판독이 가능한 형식으로 볼 수 없다. 예를 들어 아이콘이 물리적 문서, IoT 장치 또는 IoT 장치의 포장, 공공장소의 Wi-Fi 추적에 대한 고지, QR 코드, CCTV 고지에 제시되는 등 아이콘이 전자적으로 제시되지 않는 상황도 있을 수 있다.

나. 정보주체의 접근권(열람권)

정보주체는 자신과 관련된 개인정보가 처리되고 있는지 여부에 대해 컨트롤러로부터 확인을 받을 수 있는 권리를 가진다. 이러한 정보주체의 접근(열람) 요구가 있을 경우 처리 목적, 관련된 개인정보의 유형(category), 개인정보를 제공받았거나 제공받을 수령인 또는 수령인의 범주, 가능하다면 개인정보의 예상 보유기간 또는 가능하지 않다면 해당

기간을 결정하기 위하여 이용되는 기준, 컨트롤러에게 본인의 개인정보에 대한 수정·삭제 또는 처리 제한이나 처리에 대한 반대를 요구할 수 있는 권리의 유무, 감독기구에 민원을 제기할 수 있는 권리, 개인정보가 정보주체로부터 수집되지 않은 경우 개인정보의 출처에 대한 모든 가용한 정보에 대하여 접근(열람)할 수 있도록 조치하여야 한다(제15조 제1항).

개인정보가 제3국이나 국제기구에 이전되는 경우, 정보주체는 적정한 안전조치에 의한 이전 규정(GDPR 제46조)에 따라 적절한 안전조치에 대한 정보를 고지받을 권리를 가진다(제15조 제2항).

컨트롤러는 처리가 진행 중인 개인정보의 사본을 무상으로 제공하는 것을 원칙으로 하며, 정보주체가 추가 사본을 요청하는 경우에는 컨트롤러는 행정적 비용에 근거하여 합리적인 비용을 청구할 수 있다. 정보주체가 전자적 방식으로 요청을 하는 경우, 관련 정보는 통상적으로 사용되는 전자적 양식으로 제공되어야 한다(제15조 제3항). 이처럼 컨트롤러는 정보주체가 자신의 개인정보에 대한 접근(열람)권을 쉽게 행사할 수 있도록 관련 절차와 양식(form)을 제공하여야 한다. 가능한 한 컨트롤러는 정보주체가 안전한 시스템을 통하여 자신의 개인정보에 직접 원격으로 접속할 수 있도록 하여야 한다. 또한 컨트롤러는 접근(열람)을 요청한 정보주체의 신원확인을 위하여, 특히 온라인 서비스의 제공 및 온라인 식별과 관련하여 합리적인 모든 수단을 활용할 수 있지만, 컨트롤러는 잠재적 요청(potential request)의 응대라는 유일한 목적만으로 개인정보를 보유해서는 안 된다(전문 64).

한편, 처리가 진행 중인 개인정보의 사본을 입수할 권리는 제3자의 권리와 자유를 침해하지 않아야 한다(제15조 제4항). 정보주체의 접근(열람)권은 영업비밀, 지식재산권, 저작권 등을 포함하여 다른 사람의 권리와 자유를 침해하여서는 안 된다. 하지만 그로 인하여 정보주체의 권리가 전체적으로 거부되어서도 안 된다.

다. 부정확한 개인정보에 대한 수정권(정정권)

정보주체는 본인에 관하여 부정확한 개인정보를 부당한 지체 없이 수정하도록 컨트롤러에게 요구할 권리를 가지며, 정보주체는 처리 목적을 참작하여 추가 진술을 제공할 수

단을 통하는 등으로 불완전한 개인정보를 보완할 권리를 가진다(제16조). 개인정보의 정확성 원칙에 따라 정보주체에게 자신에 관한 부정확한 정보를 수정(정정)하도록 요구할 권리를 가지도록 하는 것이다. 이러한 수정권은 정보주체의 개인정보를 더욱 높은 수준으로 보호하기 위한 것이다.

정보주체의 이름 철자 수정이나 주소, 전화번호 변경 등은 단순한 수정 요구만으로도 가능하다. 그러나 정보주체 본인임을 법적으로 확인하는 용도 또는 법률 문서의 송달을 위한 거주지 주소의 변경 등을 위한 경우라면, 단순한 수정 요구만으로는 가능하지 않고 컨트롤러가 기존 정보의 부정확성을 확인하기 위해 정보주체에게 일정한 증거를 요구할 수도 있게 된다. 이때 정보주체에게 불합리한 수준의 증명 부담을 지워서는 안 된다.

정보주체가 수정권을 행사하면 컨트롤러는 부당한 지체 없이 수정 요구를 받은 시점으로부터 1개월 이내에 수정을 위한 조치를 이행해야 하고, 만일 수정 요구가 복잡한 경우에는 2개월의 추가 연장이 가능하다(제12조 제3항). 컨트롤러가 수정 요구에 따른 조치를 하지 않은 경우, 정보주체에게 그 이유 및 감독기구에 민원을 제기할 수 있고 사법적 구제를 청구할 수 있음을 알려주어야 한다(제12조 제4항). 개인정보를 수령인에게 공개·제공하였다면 가능한 한 그 수령인에게 수정에 대하여 통지하여야 한다(제19조). 또한 컨트롤러는 정보주체가 요구하는 경우 그 정보의 수령인에 대한 사항을 정보주체에게 통지해 주어야 한다.

라. 삭제권(잊힐 권리)

정보주체는 본인에 관한 개인정보를 부당한 지체 없이 삭제하도록 컨트롤러에게 요청할 권리를 가진다(제17조 제1항). 정보주체가 자신에 관한 개인정보를 삭제하기를 원하는 경우, 이를 삭제할 수 있도록 하여 그에 대한 개인정보의 처리가 이루어지지 않도록 하는 권리이다. 특히 해당 개인정보가 제3자에게 공개된 경우, 제3자들에 대하여도 일정한 사항을 알리고 합리적 조치를 취하도록 할 의무를 부과하고 있다.

이에 따라 컨트롤러는 개인정보가 수집되거나 처리된 목적에 더 이상 필요하지 않은 경우, 정보주체가 처리의 기반이 되는 동의를 철회하고 해당 처리에 대한 다른 법적 근거가 없는 경우, 개인정보가 불법적으로 처리된 경우, 컨트롤러에 적용되는 유럽연합 또

는 회원국 법률에 따른 법적 의무의 준수를 위하여 삭제되어야 하는 경우, 아동에게 직접 제공되는 정보사회 서비스와 관련하여 개인정보가 수집된 경우 중 어느 하나에 해당할 경우 부당한 지체 없이 개인정보를 삭제할 의무를 부담한다.

원칙적으로 컨트롤러는 개인정보를 제공받은 각 수령인에게도 이행된 개인정보의 삭제에 대해 통지해야 한다(제19조). 예외적으로 이러한 통지가 불가능하다고 입증되거나 과도한 노력을 수반하는 경우에는 하지 않아도 된다. 컨트롤러는 정보주체의 요청이 있을 경우 정보주체에게 해당 수령인에 대한 사항을 통지해야 한다.

컨트롤러가 개인정보를 공개하였고 해당 개인정보를 삭제할 의무가 있는 경우, 컨트롤러는 가용한 기술과 비용을 고려하여 해당 개인정보를 처리하고 있는 다른 컨트롤러들에게도 정보주체가 그들에 의한 해당 개인정보에 대한 링크, 사본, 복제물의 삭제를 요청하였음을 알리기 위하여 기술적 조치 등 합리적 조치를 취하여야 한다(제17조 제2항). 디지털 인터넷 온라인 환경에서 정보주체의 잊힐 권리를 실효성 있게 보장하기 위해 구체적인 제반 조치 의무를 부여하고 있다.

한편, 컨트롤러에게 일정한 경우에는 정보주체의 삭제 요구를 거부할 수 있도록 하고 있다(제17조 제3항). 표현 및 정보의 자유에 관한 권리행사를 위한 경우, 유럽연합 또는 회원국 법률에 따른 법적 의무를 준수하거나 공익을 위한 직무 수행을 위한 경우, 컨트롤러에게 부여된 공적 권한의 행사를 위한 경우, 공중보건 분야의 공익을 위한 경우, 공익을 위한 기록보존, 과학적·역사적 연구 또는 통계 목적을 위한 것인 경우로서 삭제권의 행사가 불가능하다고 생각되거나 삭제권의 행사로 해당 처리의 목적 달성을 심각하게 저해할 가능성이 있는 경우, 법적 권리의 확립 및 행사나 방어를 위한 경우로서 개인정보의 처리가 필요한 경우에는 정보주체의 삭제권은 적용되지 않는다.

마. 개인정보의 처리에 대한 제한권

정보주체는 자신에 관한 개인정보의 처리에 대해 제한할 권리를 갖는다(제18조 제1항). 정보주체가 개인정보의 처리에 대한 제한권을 행사하면 컨트롤러는 그 정보를 보유만 할 수 있고, 이용 및 제공 등의 처리는 제한된다. 이러한 정보주체의 개인정보 처리에 대한 제한권은 주로 개인정보의 정확성, 처리의 합법성 등에 대하여 분쟁이 있거나 소송 수행

등을 위하여 보존의 필요성이 있는 경우에 이용을 제한하면서 삭제를 보류할 수 있도록 요구할 수 있는 권리이다.

이에 따라 정보주체는 컨트롤러가 개인정보의 정확성을 증명할 수 있는 기간 동안 정보주체가 해당 개인정보의 정확성에 대해 이의를 제기하는 경우, 처리가 불법적이고 정보주체가 해당 개인정보의 삭제에 반대하고 대신 개인정보에 대한 이용의 제한을 요청하는 경우, 컨트롤러가 처리 목적을 위해 해당 개인정보가 더 이상 필요하지 않지만, 컨트롤러가 법적 권리의 확립, 행사, 방어를 위해 요구하는 경우, 컨트롤러의 정당한 이익이 정보주체의 정당한 이익에 우선하는지 여부를 확인할 때까지, 정보주체가 프로파일링 등(제21조 제1항에 따른) 처리에 대해 반대하는 경우 중 어느 하나에 해당하면, 컨트롤러의 처리를 제한할 권리를 가진다(제18조 제1항).

또한 원칙적으로 컨트롤러는 개인정보를 제공받은 각 수령인에게도 해당 개인정보의 처리 제한에 대해 통지해야 하며, 컨트롤러는 정보주체의 요청이 있을 경우 정보주체에게 해당 수령인의 사항에 대해 통지해야 한다(제19조).

개인정보 처리를 제한하는 방법에는 선택된 정보를 임시로 다른 처리시스템으로 이전하는 방법, 이용자가 선택된 정보를 열람하지 못하게 하거나 공개된 개인정보를 웹사이트에서 임시로 제거하는 방법 등이 포함될 수 있다(전문 67).

이처럼 개인정보의 처리가 제한되는 경우라도, 보관을 제외한 해당 개인정보는 정보주체의 동의가 있는 경우, 법적 권리의 확립, 행사 및 방어를 위한 경우, 제3자나 법인의 권리를 보호하기 위한 경우, 유럽연합 또는 회원국의 중요한 공익상의 이유에 해당되는 경우 중에서 어느 하나에 해당하면 처리될 수 있다(제18조 제2항). 컨트롤러는 개인정보 처리 제한을 해제할 것으로 결정한 경우, 그 사실을 처리 제한권을 가진 정보주체에게 고지해야 한다(제18조 제3항).

2. 미국 CCPA의 정보주체의 권리

미국의 경우 개인정보 보호에 관한 연방정부 차원의 공공부문과 민간부문을 포괄한 일반법은 존재하지 않는다. 연방정부의 개인정보 처리 행위를 규율하는 국가적 입법의 하나로 프라이버시법(The Privacy Act of 1974)이 있다. 미국의 개인정보 보호 체계는 기

본적으로 시장 자율 규제(self-regulation) 방식에 기초하므로, GDPR이나 우리나라의 개인정보 보호법과 같이 공공부문과 민간부문을 포괄하는 종합적인 법률은 존재하지 않는다. 연방 법률에는 공공, 금융, 통신, 교육, 의료, 비디오 감시, 근로자 정보 등 영역별 개인정보 보호 관련 법규가 있으며, 각 주(州) 단위로 프라이버시 보호 관련 법률이 있다.

미국 캘리포니아 소비자 프라이버시 보호법(The California Consumer Privacy Act of 2018: CCPA)은 미국 헌법상 프라이버시 권리를 증진하고, 소비자의 개인정보와 관련된 기존 법률을 보충하고자 하는 것으로, 소비자에게 개인정보를 효과적으로 관리할 수 있는 방법을 제공함으로써 개인정보 보호 권리를 증진하는 목적을 가진다.

CCPA는 개인정보 보호를 위하여 소비자에게 개인정보 수집 등에 대한 공개 요구권(정보를 제공받을 권리), 접근권, 삭제 요구권, 옵트아웃권(사후적 판매거부권), 개인정보 이동권, 권리행사를 이유로 한 차별을 받지 않을 권리를 인정하고 있다.

소비자는 사업자에게 본인의 개인정보 수집 등에 대한 공개 요구권을 가진다. 소비자는 개인정보를 수집하는 사업자에게 수집한 개인정보의 범주, 수집한 개인정보의 출처, 개인정보를 수집 판매하기 위한 사업적 상업적 목적, 제3자와 개인정보를 공유하는 경우 해당 제3자의 범주, 사업자가 소비자에 대해 수집한 개인정보의 특정 부분을 공개(disclose)할 것을 요구할 권리가 있다(CCPA §1798.110(a)). 소비자는 개인정보를 제3자에게 판매하거나 업무상 목적으로 공개하는 사업자에게 수집한 개인정보의 범주, 판매한 개인정보의 범주 및 판매한 제3자의 범주, 업무상 목적으로 공개한 개인정보의 범주에 대한 사항을 소비자에게 공개할 것을 요청할 수 있는 권리가 있다(§1798.115(a))[179].

소비자는 개인정보를 제3자에게 판매하는 사업자에 대해 자신의 개인정보를 판매하지 말 것을 지시할 권리인 '옵트아웃권(right to opt out)'을 가진다(§1798.120(a)). 제3자에게 소비자의 개인정보를 판매하는 사업자는 소비자에게 개인정보가 판매될 수 있으며, 이에 대해 소비자는 자신의 개인정보 판매를 옵트아웃 할 수 있는 권리를 갖는다는 내용의 고지(notice)를 소비자에게 제공해야 한다(§1798.120(b)). 소비자 또는 소비자가 승인한 자가 소비자 개인정보의 판매를 옵트아웃 할 수 있는 인터넷 웹페이지에 "내 개인정보를 판매하지 말 것"이라는 제목으로 명확하고 눈에 띄는 링크를 제공해야 한다(§1798.130(a)(2))[180].

179) 한국인터넷진흥원(2018), 앞의 글, p162.

이러한 옵트아웃 규정에도 불구하고 사업자가 16세 미만으로부터 수집한 개인정보를 판매하고자 하는 경우, '옵트인 동의(opt-in consent)'가 필요하다(§1798.120(d)). 이때 13세에서 16세 미만의 개인정보인 경우에는 정보주체 본인의 옵트인 동의가 필요하고, 13세 미만의 개인정보인 경우에는 정보주체의 부모나 후견인의 옵트인 동의가 필요하다.

소비자는 사업자가 소비자로부터 수집한 소비자의 개인정보를 삭제(delete)하도록 사업자에게 요구할 수 있는 권리를 가진다(§1798.105(a)). 이에 따라 소비자로부터 개인정보 삭제 요구를 받은 사업자는 소비자의 개인정보를 기록에서 삭제해야 하며, 모든 서비스 제공업체(service provider)에 대해 해당 소비자의 개인정보를 삭제할 것을 지시해야 한다(§1798.105(c)). 사업자는 소비자에게 본인의 개인정보를 삭제할 권리가 있다는 것을 알려주어야 한다(§1798.105(b)). 예외적으로 사업자 또는 서비스 제공업체는 소비자의 개인정보가 거래를 완료하거나 소비자와의 지속적 업무 관계 맥락상 합리적으로 예상된 상품 및 서비스를 제공하거나, 해당 계약을 이행하기 위한 목적을 위한 경우, 법률의 준수, 역사적 및 통계적 연구에 필요한 경우에는 소비자의 삭제 요구를 따르지 않을 수 있다(§1798.105(d))[181].

사업자는 소비자의 개인정보 수집 등에 대한 공개 요구권, 옵트아웃권, 삭제 요구권에 대한 사항을 준수하기 위해 소비자의 개인정보에 대한 접근권을 보장하는 조치를 해야 한다. 소비자의 공개 요구에 따른 회신을 위한 한 가지 이상의 방법으로, 직전 12개월 내 수집했던 개인정보 범주의 목록, 직전 12개월 내 판매했던 개인정보 범주의 목록, 직전 12개월 내 사업자가 소비자에 대해서 공개했던 개인정보 범주의 목록 등의 정보를 공개하고, 해당 정보를 12개월마다 최소한 한 번 업데이트해야 한다. 또한 온라인 개인정보 보호정책을 보유하고 있는 경우, 해당 온라인 개인정보 보호정책과 캘리포니아 소비자 개인정보 보호 권리 내역에 정보를 공개해야 하고, 사업자가 온라인 개인정보 보호정책을 보유하고 있지 않은 경우에는 인터넷 웹 사이트에 정보를 공개해야 한다[182].

사업자는 소비자가 개인정보 보호를 위한 권리를 행사했다는 이유로 소비자를 차별해서는 안 된다(§1798.125). 이때 소비자를 차별하는 방법으로는 소비자에게 상품이나 서비스를 제공하는 것을 거부하는 행위, 할인이나 기타 혜택을 이용하거나 벌칙을 부과하

180) 한국인터넷진흥원(2018), 앞의 글, p163.
181) 한국인터넷진흥원(2018), 앞의 글, p164.
182) 한국인터넷진흥원(2018), 앞의 글, p164.

는 방식을 포함하여 상품이나 서비스에 대해 다른 가격이나 요율을 부과하는 행위, 다른 수준이나 품질의 제품 또는 서비스를 제공하는 행위, 소비자가 상품이나 서비스에 대해서 다른 가격이나 요율을 받거나 다른 수준이나 품질의 제품 또는 서비스를 받을 것이라고 암시하는 행위가 해당된다[183].

3. 일본 개인정보 보호법의 정보주체의 권리

일본의 개인정보 보호법은 정보주체 본인의 개인정보 취급 사업자에 대한 식별 보유 개인정보의 공개 청구권, 개인정보 내용의 정정·추가·삭제 청구권, 개인정보의 이용 정지 또는 삭제 청구권, 개인정보의 제3자에 대한 제공정지 청구권, 정보주체의 개인정보에 대한 조치 요구 또는 청구에 대해 개인정보 취급 사업자가 취한 조치의 이유에 대한 설명을 요구하는 권리가 인정된다.

정보주체 본인은 개인정보 취급 사업자에 대하여 당해 본인이 식별되는 보유 개인정보의 공개를 청구할 수 있다(제28조 제1항). 정보주체의 개인정보 공개 청구를 받은 때에, 개인정보 취급 사업자는 본인에게 정령으로 정하는 방법에 따라 지체 없이 해당 보유 개인정보를 공개해야 한다(제28조 제2항). 그러나 본인 또는 제3자의 생명, 신체, 재산 기타의 권리 이익을 해칠 우려가 있는 경우, 해당 개인정보 취급 사업자의 업무의 적정한 실시에 현저한 지장을 미칠 우려가 있는 경우, 다른 법령에 위반하게 되는 경우 중 어느 하나에 해당하는 경우는 그 전부 또는 일부를 공개하지 않을 수 있다.

정보주체 본인은 개인정보 취급 사업자에 대하여 당해 본인이 식별되는 보유 개인정보의 내용이 사실이 아닐 경우, 당해 보유 개인정보 내용의 정정, 추가 또는 삭제를 청구할 수 있다(제29조 제1항). 정보주체 본인의 정정, 추가 또는 삭제 청구를 받은 개인정보 취급 사업자는 그 내용의 정정 등에 관하여 다른 법령의 규정에 특별 절차가 정해져 있는 경우를 제외하고는, 이용 목적의 달성에 필요한 같은 범위 내에서 지체 없이 필요한 조사를 실시해, 그 결과에 따라 해당 보유 개인정보 내용의 정정 등을 해야 한다(제29조 제2항). 개인정보 취급 사업자는 정보주체 본인의 정정, 추가 또는 삭제 청구에 관련된 보유 개인정보 내용의 전부 또는 일부에 대하여 정정 등을 했을 경우 또는 정정

183) 한국인터넷진흥원(2018), 앞의 글, pp164-165.

등을 하지 않는 취지의 결정을 한 경우, 정보주체 본인에 대해 지체 없이 그 취지(정정 등을 한 경우는 그 내용을 포함)를 통지하여야 한다(제29조 제3항).

정보주체 본인은 당해 본인이 식별되는 보유 개인정보가 이용 목적에 의한 제한 규정을 위반하여 취급되고 있는 경우 또는 적정한 취득의 규정(허위, 기타 부정한 수단에 의한 개인정보 취득 금지)을 위반하여 취득된 것일 경우, 개인정보 취급 사업자에 대하여 당해 보유 개인정보의 이용 정지 또는 삭제를 청구할 수 있다(제30조 제1항). 정보주체 본인은 당해 본인이 식별되는 보유 개인정보가, 미리 본인의 동의를 얻지 않고 개인정보를 타인에게 제공하는 것을 금지하는 규정을 위반하는 경우 또는 미리 본인의 동의를 받지 않고 외국에 있는 제3자에게 개인정보를 제공하는 것을 제한하는 규정을 위반하여 타인에게 제공되는 때에는, 개인정보 취급 사업자에 대하여 당해 보유 개인정보의 제3자에 대한 제공의 정지를 청구할 수 있다(제30조 제3항).

개인정보 취급 사업자는 정보주체 본인의 보유 개인정보에 대해 본인으로부터 요구 또는 청구 조치의 전부 또는 일부에 대하여 그 조치를 하지 않는 취지를 통지하는 경우, 또는 그 조치와 다른 조치를 할 것이라는 취지의 통지를 하는 경우는 본인에게 그 이유를 설명하도록 노력하여야 한다(제31조).

4. 우리나라 개인정보 보호법의 정보주체의 권리

우리나라 개인정보 보호법에서 정보주체는 자신의 개인정보 처리와 관련하여 개인정보의 처리에 관한 정보를 제공받을 권리, 개인정보의 처리에 관한 동의 여부 및 동의 범위 등을 선택하고 결정할 권리, 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함)을 요구할 권리, 개인정보의 처리 정지와 정정·삭제 및 파기를 요구할 권리, 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리를 가진다(제4조). 그리고 개인정보의 열람권(제35조), 개인정보의 정정·삭제권(제36조), 개인정보의 처리정지요구 및 파기권(제37조)을 구체적으로 규정하고 있다.

정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다(제35조 제1항). 정보주체가 자신의 개인정보에 대한 열람을 공공기관에 요구하고자 할 때에는 공공기관에 직접 열람을 요구하거나 대통령령으로 정

하는 바에 따라 보호위원회를 통하여 열람을 요구할 수 있다(제35조 제2항). 개인정보처리자는 열람을 요구받았을 때에는 10일 내에 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 하며, 이 경우 해당 기간 내에 열람할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며, 그 사유가 소멸하면 지체 없이 열람하게 하여야 한다(제35조 제3항).

개인정보처리자는 법률에 따라 열람이 금지되거나 제한되는 경우, 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우, 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다(제35조 제4항 제1호 및 제2호). 또한 공공기관이 조세의 부과·징수 또는 환급에 관한 업무, 「초·중등교육법」 및 「고등교육법」에 따른 각급 학교, 「평생교육법」에 따른 평생교육시설, 그 밖의 다른 법률에 따라 설치된 고등교육기관에서의 성적 평가 또는 입학자 선발에 관한 업무, 학력·기능 및 채용에 관한 시험, 자격 심사에 관한 업무, 보상금·급부금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무, 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무의 어느 하나에 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다(제35조 제4항 제3호).

자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다(제36조 제1항). 개인정보처리자는 개인정보의 정정 또는 삭제에 따른 정보주체의 요구를 받았을 때에는 개인정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다(제36조 제2항). 이에 따라 개인정보처리자가 개인정보를 삭제할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다(제36조 제3항). 개인정보처리자는 정보주체의 요구가, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우 그 삭제를 요구할 수 없는 경우에 해당될 때에는 지체 없이 그 내용을 정보주체에게 알려야 한다(제36조 제4항). 개인정보처리자는 제2항에 따른 조사를 할 때 필요하면 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있

다(제36조 제5항).

정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있고, 이 경우 공공기관에 대하여는 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다(제37조 제1항). 개인정보처리자는 개인정보에 대한 처리의 정지 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다(제37조 제2항). 그러나 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우, 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우, 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다(제37조 제2항 단서). 이에 따라, 개인정보처리자는 처리정지 요구를 거절하였을 때에는 정보주체에게 지체 없이 그 사유를 알려야 한다(제37조 제3항). 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다(제37조 제4항).

5. 개선방안

우리나라 개인정보 보호법의 정보주체의 권리는 대체로 GDPR의 정보주체의 권리와 유사하며, CCPA와 일본 개인정보 보호법의 정보주체의 권리의 내용도 포함하고 있는 것으로 볼 수 있다. 하지만 정보주체의 권리행사를 보장하기 위한 구체적인 방법에 있어 차이가 있다.

가장 큰 문제는 실제에 있어 우리나라 개인정보 보호법에 규정된 정보주체의 권리는 그 행사가 거의 이루어지고 있지 않다는 점이다. 그 이유는 정보주체가 자신이 행사할 수 있는 권리가 무엇이며, 그 내용은 무엇인지를 제대로 인식하지 못하고 있는 것이 가장 큰 요인으로 생각된다. 이것은 정보주체의 권리행사를 보장하고 실행할 수 있도록 하기 위한 법규범이 미흡한 점에서부터 비롯한다. 이에 대한 개선을 위해, 특히 GDPR의

정보주체의 권리행사를 위한 투명한 정보, 통지 및 형식에 대한 규정을 참조하여 우리 법에도 규정함으로써 개인정보 처리 정보를 제공받을 권리를 실효성 있게 강화할 필요가 있다. 우리나라 개인정보 보호법은 정보주체의 동의를 받을 때에만, '알아보기 쉽게 표현' 하라고 규정되어 있을 뿐이다. 따라서 동의에서부터 처리에 이르기까지, 정보주체에게 자신의 권리 및 행사 방법을 고지하고, 정확하고 투명하며 이해하기 쉬운 형식으로 명확하고 평이한 언어를 사용하여 제공할 것을 명확히 규정할 필요가 있다. 열람, 정정, 삭제권 등 정보주체가 행사할 수 있는 권리의 존재 및 권리행사 방법, 향후 동의를 철회할 수 있는 권리, 감독기관에 민원을 제기할 수 있는 권리, 처리의 법적 근거, 개인정보를 제공할 의무가 있는지 여부, 위탁할 경우 위탁자 및 위탁의 내용(현재 개인정보처리방침에만 공개하도록 하고 있음) 등 정보주체의 권리행사 등을 위해 필요한 항목에 대한 내용 측면에서의 개선이 필요하다.

우리나라 개인정보 보호법은 개인정보의 처리 여부를 확인하고 개인정보에 대하여 사본의 발급을 포함한 열람을 요구할 권리를 보장하며(제4조), 구체적으로는 처리하는 자신의 개인정보에 대한 열람을 보장한다(제35조). 하지만, '개인정보의 처리 여부 및 처리의 방법' 이 열람권의 대상으로 제35조에 명시되어 있지 않다는 점은 문제이다. 따라서 이 경우에도 정보주체 자신의 개인정보의 처리 및 처리자가 보유하고 있는 개인정보, 정보주체의 권리 및 행사 방법 등 모든 관련 정보를 열람할 수 있도록 개선해야만 한다. 또한 열람권 행사를 위해서는 개인정보처리자가 서면, 전화, 전자우편, 인터넷 등 정보주체가 쉽게 활용할 수 있는 방법으로 제공하며 인터넷 홈페이지에 열람 요구 방법과 절차를 명시하는 등의 방법으로 이루어지도록 하고 있다. 그 방법의 제공에 있어서는 GDPR이나 CCPA와 거의 같다. 그러나 GDPR과 CCPA는 정보주체의 접근 및 열람의 편의성을 더욱 강하게 보장하는 방법을 취하여, 정보주체가 원하는 방식으로 정보주체의 권리행사에 관한 정보를 제공하도록 규정한다. 이러한 방식은 개인정보처리자가 제공하는 방법과 절차에 의해 정보주체가 열람권을 행사하도록 하는 우리나라 법과 크게 다른 점이다.

우리나라의 개인정보 보호법에서 어떤 경우에는 개인정보처리자가 마련한 방법과 절차를 따르도록 하고 있고, 어떤 경우에는 고시에서 정하는 바에 따라 요청 또는 답변을 하도록 하고 있다. 예를 들어, 고시 제3조 제6항 별지 제8호 서식 <개인정보 열람요구

서>는 보호위원회를 통해 공공기관에 열람을 요구하는 경우에 사용하는 서식이고, 고시 제3조 제6항 별지 제9호 서식 <열람의 연기·거절 통지서>는 모든 개인정보처리자로 되어 있다. 이것은 시행령에서 규정하고 있는 것이기는 하지만, 열람요구서와 열람의 연기·거절 통지서의 적용 범위가 다른 것이 다소 혼란을 초래할 수 있다. 또한 공공기관이 아닌 일반 개인정보처리자의 경우 스스로 마련한 방법과 절차에 따라 열람 청구, 정정·삭제 청구를 받고 있는데, 열람 통지, 연기·거절 통지 등은 고시에서 정한 서식으로 하도록 하고 있다. 또한 이러한 서식에 따르지 않았을 경우 어떻게 되는지도 모호하다. 규제기관이 하나의 예시로 서식 등을 제시할 수는 있다. 하지만, 서식의 형식과 상관없이, 정보주체의 권리행사 등을 위해 필요한 항목 등의 내용을 서식에 반드시 포함하도록 하는 방식으로 개인정보 보호법에 규정하는 것이 바람직하다.

한편 우리나라 개인정보 보호법에서는 동의를 받을 때에만 정보주체에게 개인정보 수집·이용 목적 등 일부 내용을 고지하도록 하고 있는데, 다른 적법 근거(계약, 법률에 근거 혹은 정당한 이익 등)에 따라 개인정보를 수집할 경우에도 정보주체에게 관련 사항을 고지하도록 개선해야 할 것이다. 또한 고지하는 내용이 너무 제한적이므로 열람, 정정, 삭제권 등 정보주체가 행사할 수 있는 권리의 존재 및 권리행사 방법, 감독기관에 민원을 제기할 수 있는 권리 등 정보주체의 권리에 대한 내용들도 고지 내용에 포함되도록 하는 것이 바람직하고 필요하다.

정보주체에게 직접 개인정보를 수집하지 않는 경우, 우리나라 개인정보 보호법은 '정보주체의 요구가 있을 경우에만' 수집 목적 등 관련 내용을 알리도록 하고 있을 뿐만 아니라 동의가 아닌 다른 법적 근거에 의해 제3자에 제공되는 경우 제공하는 처리자 및 제공받는 처리자가 모두 관련 사항을 고지할 의무가 없다는 점도 문제이다. 또한 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자가 정보주체 이외로부터 개인정보를 수집하여 처리하는 때에는 개인정보의 수집 출처, 처리 목적, 개인정보 처리의 정지를 요구할 권리가 있다는 사실을 정보주체에게 알려야 하는데, 이 경우에도 정보주체의 동의를 받아 수집하는 경우에만 적용될 뿐이므로, SNS등 공개된 개인정보를 수집하거나 다른 적법 근거에 따라 다른 소스로부터 개인정보를 수집했을 경우에는 적용되지 않는 문제가 있다. 따라서 GDPR처럼 정보주체에게 직접 개인정보를 수집하지 않는 경우에도, 고지가

현실적으로 불가능한 예외적인 경우가 아니라면, 주요 개인정보 처리 내용을 고지하도록 개선할 필요가 있다.

더 나아가서 정보주체의 권리를 더욱 강하게 보장하고 그 행사를 실효성 있게 하기 위해서는 정보주체의 권리행사의 편의성을 더욱 높이는 방법과 절차를 강구해야 할 필요성이 있다. 급속하게 변화하는 디지털 환경에서 개인정보 처리 등 관련 정보와 권리에 대한 제공 방법 및 절차에 있어 정보주체의 가독성과 편의성을 높일 수 있도록 하는 방안을 모색해야만 정보주체의 권리가 실효성 있게 보장될 수 있을 것이다. 개인정보 처리 방침 등을 사이트 홈페이지에 게시하고 있으나, 이러한 방식만으로는 정보주체의 권리보장 및 행사를 실효성 있게 하지 못한다. 정보주체가 가입하여 개인정보 처리 등에 대한 동의 절차 등을 거친 후에, 개인정보처리자가 정보주체에게 보장되어 있는 권리들을 쉽고 간단한 문구를 사용하여 이메일, 메시지, 앱의 알림 등 정보주체가 원하는 방법으로 알려주도록 강제하여야 한다. 그리고 이러한 권리 내용에 대한 제공은 그 권리와 관련된 사항이 발생했을 때 직접 관련되는 권리 내용을 고지하는 것은 물론이고, 정기적으로도 알려주도록 하는 방법도 강구할 필요가 있다. 또한 해당 정보주체가 자신의 권리 및 그 행사 등에 대해서 묻고, 이에 답변할 수 있는 방법(예를 들어, 상담 채팅 등의 활용)도 개인정보처리자에게 마련하도록 할 필요가 있다.

우리나라는 정보주체가 자신의 개인정보를 열람한 후에 정정권 및 삭제권을 부여하는 방식을 취하고 있다. 반면 GDPR, CCPA, 일본 개인정보 보호법 그 어디에도 그러한 방식을 취하고 있지 않다. 정정권 및 삭제권의 행사를 열람권의 행사를 전제로 할 경우, 정보주체의 권리행사에 넘어야 할 장애물을 하나 더 설치하는 것과 같은 효과를 가지게 되므로 이를 개선하는 것이 바람직하다.

우리나라는 정보주체가 자신의 개인정보 처리의 정지를 요구할 수 있는 조건을 제한하고 있지 않으며, 처리 전체에 대한 정지 및 처리의 일부 정지도 가능하게 하고 있다. GDPR은 정보주체의 처리에 대한 제한권은 처리자가 개인정보를 보유는 하며 개인정보의 처리 전체를 하지 못하도록 하고, 제18조 제1항 (a)호부터 (d)호까지에 해당하는 경우 처리 제한권을 부여하고 있다. 우리나라의 처리정지권이 GDPR보다 넓게 인정되고 있다. 하지만, 그러한 처리정지권이 현실적으로 거의 활용되고 있지 않다는 점이 문제로 지적된다. 따라서 이러한 정보주체의 처리정지권도 앞서 논한 것과 마찬가지로, 그 행사 및

방법을 실효성 있도록 하는 절차와 내용이 필요하다.

또한 GDPR은 정보주체의 삭제권, 처리 제한권 행사의 예외로 “법적 권리의 확립, 행사 또는 방어를 위한 경우”를 규정하고 있다. 이러한 예외 규정은 우리나라에도 도입할 필요가 있는 것으로 보인다.

제3절 정보주체의 개인정보 이동권

1. GDPR의 정보주체의 개인정보 이동권

개인정보 이동권은 정보주체의 개인정보를 어느 한 IT 환경에서 다른 곳으로 쉽게 이동, 복사, 전송할 수 있도록 정보주체에게 권한을 주는 것을 주요 내용으로 한다. 실제에 있어 개인정보 이동권의 기본적인 목적은 하나의 서비스 제공업체에서 다른 업체로의 전환을 활성화하여 개인들이 각기 다른 공급업체들 사이에 전환을 쉽게 할 수 있게 함으로써, 서비스업체들 사이의 경쟁을 강화하고 디지털 단일시장 전략의 맥락에서 새로운 서비스를 창출할 수 있도록 하기 위한 것이다[184].

정보주체는 컨트롤러에게 제공한 본인에 관련된 개인정보를 체계적이고 통상적으로 사용되며 기계 판독이 가능한 형식으로 수령할 권리가 있으며, 개인정보를 제공받은 컨트롤러로부터 방해받지 않고 다른 컨트롤러에게 해당 개인정보를 이동할 권리를 가진다(제20조 제1항). 이에 따라 본인의 개인정보 이동권을 행사하는 데 있어, 정보주체는 기술적으로 가능한 경우 해당 개인정보를 한 컨트롤러에서 다른 컨트롤러로 직접 이동할 권리를 가진다(제20조 제2항).

이러한 정보주체의 개인정보 이동권은 처리한 개인정보를 컨트롤러로부터 받을 수 있는 권리와 개인정보를 한 컨트롤러로부터 다른 컨트롤러에게 전송할 수 있는 권리의 두 가지로 구성된다. 또한 개인정보 이동권은 처리가 정보주체의 동의나 계약을 근거로 하는 경우와 처리가 자동화된 수단으로 시행되는 경우 적용된다. 따라서 개인정보의 처리가 동의 또는 계약 이외의 법적 사유를 근거로 하는 경우로 공공의 이익을 위하여 컨트롤러가 처리하는 개인정보에 대해서는 이동권이 인정되지 않게 된다.

184) ARTICLE 29 DATA PROTECTION WORKING PARTY(2017a), p3-4.

개인정보 이동권의 대상은 오직 개인정보만 있으므로, 익명이거나 정보주체와 관련이 없는 정보는 이 범주에 속하지 않는다. 그러나 정보주체에 분명하게 연결될 수 있는 가명 개인정보는 대상에 속하게 된다. 정보주체가 온라인 양식으로 제출한 계정 개인정보, 예를 들어 메일 주소, 사용자 이름, 연령 등과 같이 공공연하게 적극적으로 제공한 것은 개인정보 이동권의 범위에 포함된다. 서비스나 기기 사용을 통해 정보주체가 제공하거나 관찰된 개인정보, 예를 들어 개인의 검색 이력, 트래픽 개인정보 및 위치 개인정보도 포함될 수 있다. 또한 피트니스나 건강 추적기를 통해 추적된 심박수와 같은 개인정보도 포함될 수 있다[185].

추론된 개인정보(inferred data)와 파생된 개인정보(derived data)는 정보주체가 제공한 개인정보를 기반으로 해서 컨트롤러에 의해 만들어지는 것이므로, 이러한 개인정보들은 개인정보 이동권의 범주에 포함되지 않는다. 예를 들어 어떤 사용자의 신용점수 또는 건강과 관련한 평가 결과는 추론된 개인정보의 전형적인 예이다. 따라서 개인정보 처리의 일부로서 컨트롤러가 창출한 개인정보, 예를 들어 사용자 범주화 또는 프로파일링으로 만들어진 개인정보는 정보주체가 제공한 개인정보로부터 추론되거나 파생된 개인정보이므로 개인정보 이동권의 대상에서 제외된다[186].

정보주체의 개인정보 이동권의 행사는 삭제권(제17조)을 침해하지 않아야 한다(제20조 제3항). 정보주체의 개인정보 이동권의 행사는 자신이 제공한 개인정보의 삭제를 의미하는 것이 아니기 때문이다. 또한 이동권은 공익상의 업무를 수행하기 위하여 또는 컨트롤러에게 부여된 공적 권한의 행사를 위하여 필요한 처리에는 적용되지 않는다. 이동권은 다른 개인의 권리와 자유를 침해하지 않아야 하므로(제20조 제4항), 개인정보 이동권으로 인해 지식재산권이나 영업비밀 등 다른 사람의 권리가 침해되는 경우 이동권에 대한 의무가 적용되지 않는다.

특히 컨트롤러는 일반적으로 완전성 및 기밀성에 따라 적절한 기술적, 조직적 수단을 이용해 무허가 또는 불법적인 처리와 돌발적인 손실, 파괴 또는 손상으로부터의 보호를 비롯한 개인정보의 적절한 보안을 보장해야만 한다. 개인정보의 이동성은 컨트롤러의 정보 시스템으로부터 개인정보를 얻는 것이므로, 전송하는 동안 개인정보 침해행위가 발생

185) Ibid., pp9-10.
186) Ibid., p10.

하는 등과 같이 전송은 개인정보와 관련하여 위험의 원천이 될 수도 있다. 따라서 컨트롤러는 추가적인 인증 정보의 사용 등을 통해 개인정보가 정확하고, 안전하게 전송될 수 있도록 보장하는 모든 보안 수단을 마련해야 할 책임이 있다. 이러한 보안 수단은 사용자에게 추가 비용을 부과하는 등으로 사용자의 권리행사를 방해하는 것이어서는 안 된다[187].

온라인 서비스에서 개인정보를 가져오는 경우, 사용자가 온라인 서비스에서 제공하는 시스템보다 보안 수준이 낮은 시스템에 데이터를 저장할 수 있는 위험이 있다. 개인정보를 요청하는 정보주체는 자신의 시스템에서 개인정보를 보호하기 위해 올바른 조치를 취할 책임이 있다. 그리고 정보주체는 제공받은 정보를 보호하기 위한 조치를 취해야 한다는 사실을 인식하고 있어야 한다. 이를 위해 컨트롤러가 정보주체에게 도움이 되는 적절한 형식, 암호화 도구 및 기타 보안 조치를 권장할 수 있도록 하는 것이 실효적인 방안이 될 것이다[188].

2. 미국 CCPA의 개인정보 이동권

미국은 2011년부터 연방정부 주도하에 스마트 공개정책(Smart Disclosure Policy)을 민관협력체계를 통해 시행하여 소비자의 개인정보 이동성을 구현하고 있다. 공공기관과 민간의 기업들이 보유하고 있는 소비자의 개인정보를 표준화하여 컴퓨터가 읽을 수 있는 포맷으로 소비자 개인에게 제공하고 있다. 물론 이 정책의 시행에 있어서 개인정보의 보호와 안전성 확보조치는 중요한 구성요소를 이룬다. 이러한 스마트 공개를 통해 소비자에게 힘을 실어주어 합리적인 선택을 하도록 돕고, 시장의 투명성(market transparency)을 증대시키는 정책목표를 추진하고 있다. 이때, 스마트 공개란 소비자가 현명한 결정을 내릴 수 있도록 자신의 소비와 관련한 복잡한 정보와 데이터를 표준화되고 컴퓨터가 읽을 수 있는 포맷으로 때맞추어 제공해주는 것을 말한다[189].

CCPA는 소비자의 개인정보 이동권을 접근권(right to access)의 하나로 포섭하여 부분

187) Ibid., p19.
188) Ibid., pp19-20.
189) 김서안, 이인호(2019), 유럽연합과 미국에서의 개인정보이동권 논의와 한국에의 시사점, 중앙법학 제21집 제4호, 중앙법학회, p287-288.

적으로 인정하고 있다. 소비자가 기업이 처리하는 자신의 개인정보에 대해 접근권을 행사한 경우, 기업은 해당 개인정보를 이동이 가능한 포맷으로(in a portable format), 그리고 기술적으로 허용된다면, 받은 개인정보를 다른 기업에 아무런 장애 없이 전송할 수 있도록 쉽게 이용할 수 있는 포맷으로(in a readily useable format) 제공해주어야 한다(§1798.100(d))[190]. CCPA는 개인정보 이동권을 접근권의 연장으로 보기 때문에, 접근권과 동일한 범위에서 개인정보의 이동을 보장한다. 이에 따라 CCPA의 개인정보 이동권의 대상이 되는 개인정보는, GDPR이 정보주체가 컨트롤러에게 직접 제공한 개인정보만 이동권의 대상이 되도록 한 것과 같은 제한을 받지 않으므로, 개인정보 이동권의 대상정보 범위가 더 넓을 수 있게 된다[191].

또한 CCPA의 개인정보 이동권은 접근권의 일종으로 인정되므로, 접근권에 대한 제한이 동일하게 적용된다. 따라서 개인정보 이동권은 청구하는 시점에서 12개월 전까지 수집된 정보에만 적용되는 것 등의 제한을 받게 된다. 또한 개인정보 이동권은 개인정보를 받아서 그것을 다른 기업에 방해 없이 자유롭게 전송할 수 있는 것을 주요 내용으로 하지만, GDPR처럼 다른 기업에 바로 전송되게 할 의무까지는 인정하지 않는다.

3. 우리나라 신용정보법의 개인정보 이동권

우리나라는 개인정보 이동권을 개인정보 보호법이 아닌 신용정보법에서 개인신용정보의 전송요구권으로 신설하였다. 개인인 신용정보주체는 신용정보제공·이용자 등에 대하여 그가 보유하고 있는 본인에 관한 개인신용정보를 해당 신용정보주체 본인, 본인신용정보관리회사, 대통령령으로 정하는 신용정보제공·이용자, 개인신용평가회사의 어느 하나에 해당하는 자에게 전송하여 줄 것을 요구할 수 있다(제33조의2 제1항). 한편, 개인인 신용정보주체는 전송요구를 철회할 수 있다(제33조의2 제7항).

이에 따라 개인인 신용정보주체가 전송을 요구할 수 있는 본인에 관한 개인신용정보의 범위는 ① 해당 신용정보주체(법령 등에 따라 그 신용정보주체의 신용정보를 처리하는 자를 포함)와 신용정보제공·이용자 등 사이에서 처리된 신용정보로서 신용정보제공·이

190) 김서안, 이인호(2019), 위의 글, p291.
191) 고수윤(2020), GDPR과 CCPA상 정보주체 권리에 관한 비교법적 연구, 미디어와 인격권 제6권 제1호, p92.

용자 등이 신용정보주체로부터 수집한 정보, 신용정보주체가 신용정보제공·이용자 등에게 제공한 정보, 신용정보주체와 신용정보제공·이용자 등 간의 권리·의무 관계에서 생성된 정보의 어느 하나에 해당하는 정보일 것이 요구되고, ② 컴퓨터 등 정보처리장치로 처리된 신용정보일 것, ③ 신용정보제공·이용자 등이 개인신용정보를 기초로 별도로 생성하거나 가공한 신용정보가 아닐 것의 요소를 모두 고려하여 대통령령으로 정하는 것으로 하고 있다(제33조의2 제2항).

신용정보주체 본인으로부터 개인신용정보의 전송요구를 받은 신용정보제공·이용자 등은 개인신용정보의 이용 제한에 관한 규정(제32조) 및 「금융실명거래 및 비밀보장에 관한 법률」 제4조, 「국세기본법」 제81조의13, 「지방세기본법」 제86조, 「개인정보 보호법」 제18조, 그 밖에 그러한 법률들의 규정에서 정한 규정과 유사한 규정으로서 대통령령으로 정하는 법률의 관련 규정의 어느 하나에 해당하는 법률의 관련 규정에도 불구하고 지체 없이 본인에 관한 개인신용정보를 컴퓨터 등 정보처리장치로 처리가 가능한 형태로 전송하여야 한다(제33조의2 제3항).

신용정보주체 본인이 개인신용정보의 전송을 요구하는 경우 신용정보제공·이용자 등에 대하여 해당 개인신용정보의 정확성 및 최신성이 유지될 수 있도록 정기적으로 같은 내역의 개인신용정보를 전송하여 줄 것을 요구할 수 있다(제33조의2 제4항).

개인인 신용정보주체가 전송요구를 할 때에는 신용정보제공·이용자 등으로서 전송요구를 받는 자, 전송을 요구하는 개인신용정보, 전송요구에 따라 개인신용정보를 제공받는 자, 정기적인 전송을 요구하는지 여부 및 요구하는 경우 그 주기, 그 밖에 앞서 정한 사항과 유사한 사항으로서 대통령령으로 정하는 사항을 모두 특정하여 전자문서나 그 밖에 안전성과 신뢰성이 확보된 방법으로 하여야 한다(제33조의2 제5항).

신용정보주체 본인의 전송요구(제33조의2 제3항)에 따라 개인신용정보를 제공한 신용정보제공·이용자 등은 개인신용정보의 전송 사실을 해당 신용정보주체 본인에게 통보하지 아니할 수 있다(제33조의2 제6항).

신용정보주체 본인으로부터 개인신용정보의 전송요구를 받은 신용정보제공·이용자 등은 신용정보주체의 본인 여부가 확인되지 아니하는 경우 등 대통령령으로 정하는 경우에는 전송요구를 거절하거나 전송을 정지·중단할 수 있다(제33조의2 제8항).

4. 개선방안

개인정보 이동권은 정보주체가 자신의 개인정보를 보유하고 있는 한 IT업체 등에서 다른 업체 등으로 이동할 수 있도록 정보주체에게 권리를 주는 것으로, 데이터 산업의 활성화와 경쟁 강화 및 새로운 서비스산업 등의 창출을 위한 맥락에서 고안된 것으로 볼 수 있다. 하지만 디지털 환경에서 데이터 산업의 발전과 확대에 따라 개인정보 침해의 위험도 함께 증대할 것이라는 점을 쉽게 예상할 수 있다.

GDPR은 개인정보 이동권의 행사가 삭제권을 침해하지 않아야 한다고 규정한다(제20조 제3항). 그러나 일반적으로 개인정보 이동권의 행사는 정보주체가 한 처리자로부터 탈퇴하여 개인정보를 삭제하고, 다른 처리자로 옮기는 방법으로 실현하는 것을 상정한 것이다. 우리나라 개인정보 보호법에서는 개인정보 이동권에 대한 규정이 마련되어 있지 않고, 신용정보법에서만 규정하고 있다(2021년 2월 4일 시행). 그리고 신용정보법은 신용정보주체가 해당 개인신용정보의 정확성 및 최신성이 유지될 수 있도록 정기적으로 같은 내역의 개인신용정보를 전송하여 줄 것을 요구할 수 있다는 점(제33조의2 4항)에서, 기존 처리자에 의한 처리와는 별개로 마이데이터 사업자에 대한 통합 처리 및 개인정보 유통을 고려하여 둔 규정이라는 것을 알 수 있는데, 이 점에서 GDPR이 상정하고 있는 모델과 큰 차이가 있다.

GDPR은 프로파일링 등에 의해 추론되거나 파생된 개인정보를 개인정보 이동권의 대상에서 제외함으로써 위험성을 줄이고자 하며, 특히 컨트롤러에게 일반적으로 완전성 및 기밀성에 따라 적절한 기술적, 조직적 수단을 이용해 무허가 또는 불법적인 처리와 돌발적인 손실, 파괴 또는 손상으로부터의 보호를 비롯한 개인정보의 적절한 보안을 보장하도록 하는 의무를 지움으로써 개인정보 침해의 위험성을 실효성 있게 막고자 한다.

CCPA는 개인정보 이동권을 접근권의 하나로 인정하고, 개인정보 이동권의 대상이 되는 개인정보를 이동권을 청구하는 시점에서 12개월 전까지 수집된 정보에만 한정하는 제한을 가함으로써 일정부분 개인정보 침해 위험성을 줄이고자 한다. 또한, 정보주체가 개인정보를 받아서 그것을 다른 기업에 방해 없이 자유롭게 전송할 수 있도록 하고, GDPR처럼 한 기업에서 다른 기업으로 바로 전송되게 할 의무까지는 인정하지 않음으로써 정보주체인 소비자의 개입과 결정권을 강화하고 있는 것으로 보인다.

우리나라는 신용정보법에서만 GDPR과는 취지를 달리하는 개인신용정보의 전송요구권을 규정한다. 우리나라도 4차 산업혁명에 따른 데이터 산업의 활성화 및 경쟁 강화를 표방하고 있다. 또한 그에 따른 개인정보 침해의 위험성도 증대된다. 그러나 개인정보 보호법에 일반적인 개인정보 이동권 및 규제에 관한 규정을 마련하지 않음으로써, 개인신용정보와 직접 관련이 없는 데이터 산업에서의 개인정보 전송 등에 대한 개인정보 침해의 위험에 대해 정보주체의 권리가 보장되지 못하는 한계와 문제점을 가지게 될 수 있다.

따라서 GDPR의 정보주체의 개인정보 이동권에 관한 규정과 CCPA의 일부 규정을 토대로 개인정보 보호법에 일반적인 정보주체의 개인정보 이동권을 보장하고, 그에 따른 개인정보 침해에 대한 실효성 있는 방지 및 사후규제에 관한 규정을 마련해야 한다.

제4절 프로파일링 및 자동화된 의사결정과 개인정보 주체의 권리

1. 인공지능 알고리즘에 기반한 자동화 의사결정의 공정성·중립성에 대한 논란

알고리즘(algorithm)은 소프트웨어가 데이터를 처리하여 주어진 과업을 수행하거나 문제를 해결하기 위하여 정의된 일련의 절차로, 문제 해결을 위한 논리(logic)와 문제 해결의 전략인 통제(control)를 담고 있다[192]. 이러한 알고리즘은 자동화된 의사결정을 가능하게 하며, 거의 모든 인공지능 활용 분야의 기초로 작동하고 있다. 또한, 활용되고 있는 인공지능은 빅데이터에서 패턴을 식별하는 방식으로 구체적인 작업, 예컨대 게임을 하는 것, 이미지를 인식하는 것, 또는 신원을 확인하는 것 등을 수행하는 컴퓨터 시스템을 포함한다[193]. 빅데이터를 활용한 기술은 데이터 규모와 알고리즘 시스템을 통해 구현된다.

192) 박상돈(2017), 헌법상 자동의사결정 알고리즘 설명요구권에 관한 개괄적 고찰, 헌법학연구 제23권 제3호, 한국헌법학회, p186-187.

193) Fred H. Cate & Rachel Dockery, 김태오 옮김(2018), "인공지능과 개인정보보호 : 불필요한 갈등 증가에 대한 관견(管見)", 경제규제와 법 제11권 제2호, 서울대학교 공익산업법센터, p132.

빅데이터를 활용한 기술들은 데이터에 기반한 것이기 때문에, 그 결과물들이 단순히 모두 객관적이라고 단정할 수는 없다.

빅데이터의 알고리즘 시스템은 정교한 프로세스를 사용하고 이에 데이터를 입력해야 한다. 때문에, 만일 특정한 데이터를 사용하기로 하고 그 이외의 데이터는 입력하지 않기로 결정하는 경우에는 차별적인 결과가 발생할 수 있게 된다. 알고리즘이 편향된 데이터를 반영할 가능성 있는 기술적 경우의 문제들이 제기된다. 첫째, 알고리즘 시스템의 설계자가 특정한 데이터가 의사결정에 중요하고 다른 데이터는 중요하지 않다고 결정하는 경우, 그것은 데이터 선택을 잘못한 것이 된다. 둘째, 데이터의 수집에 있어 기술적인 엄격함과 포괄성이 부족한 경우 또는 수집된 데이터에 부정확성이나 갭(gap)이 있는 경우에, 그 데이터는 불완전한 것이거나 부정확한 것, 또는 시기가 지나쳐버린 것이 된다. 셋째, 어떤 한 모델의 그룹에 대한 일련의 데이터 입력이 모집단을 나타내지 않게 되는 경우, 다른 그룹보다 특정 그룹을 선호할 수 있는 결론이 도출되는 선택의 편향성이 나타나게 된다. 넷째, 알고리즘 시스템의 출력에 있어 과거에 입력한 데이터나 결과들이 스스로 복제되도록 하는 피드백 루프(feedback loop)는 의도하지 않게 역사적 편향성을 영구화하고 촉진하게 된다[194].

알고리즘의 자동화된 의사결정 과정에는 우선순위 결정, 분류, 관련짓기, 필터링이라는 일련의 과정이 존재하게 된다. 이 과정에서 인간의 개입에 따른 오류와 편향성, 검열의 가능성 등과 같은 본질적인 차별적 성격이 투입될 수도 있게 된다. 특히 알고리즘은 정의된 명령에 따라서만 작동하는 것이 아니라, 이용하는 사람 혹은 객체와의 상호작용 속에서 끊임없이 수정 및 조정되므로 소프트웨어 개발자의 편견이나 선입견이 반영될 가능성은 항상 존재하게 된다[195].

특히 기업은 알고리즘을 가장 많이 활용하는 주체이다. 기업이 활용하는 알고리즘은 그 속성상 영리 목적의 상업성을 가지게 되며, 방법상 이윤이 극대화될 수 있는 쪽으로 알고리즘 검색 결과를 나타나게 한다. 이에 대해 현대의 소비자들은 기업에 대한 정보와

194) White House(2016), Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights, Executive Office of the President. <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf>, pp.7-8.

195) 이원태(2016), EU의 알고리즘 규제 이슈와 정책적 시사점, KISDI Premium Report 16-12호, 정보통신정책연구원, p5.

고용, 생산품에 대한 정보를 거의 모두 인터넷 검색을 통해서 획득하므로 그에 대한 의존도는 매우 높을 수밖에 없다. 구글 온라인 광고는 여성보다 남성에게 상대적으로 임금이 높은 직업 광고를 추천하는 경향이 있고, 백인보다 흑인에게 저렴한 상품 광고를 집중적으로 보여주는 경향이 높았다는 연구 결과는 구글의 온라인 광고 알고리즘이 성차별적이고 인종차별적으로 작동했음을 보여주었다[196]. '전 세계 최초로 인공지능(AI)이 심사하는 미인대회'라는 슬로건(slogan)을 내걸고 열린 온라인 국제 미인대회에서, 대회 참가자들의 프로필 사진 심사를 맡은 인공지능 프로그램 '뷰티닷에이아이(Beauty.AI)'가 백인 여성만 대회에 입선시키고, 유색인종 여성들을 전혀 입선시키지 않은 인종차별 사례도 있었다.

2016년 5월에는 미국의 IT매체 '기즈모도'가 페이스북이 특정 미국 대선후보를 낙선시키기 위해 자신의 뉴스편집 서비스 '트렌딩 토픽'의 알고리즘을 조작했다는 의혹을 제기하는 사건도 있었다. 기계학습의 알고리즘적 편견이 반영된 개인 추천시스템(personal recommendation system)이 미국 대통령 선거후보자에 대한 유권자들의 선택에 영향을 미쳤다는 주장도 제기되었다. 미국 대선 기간 중 유튜브의 인공지능 동영상 추천 시스템이 80% 이상의 동영상을 트럼프 후보에게 우호적인 결과물로 검색, 추천하였는데, 이 추천의 대부분이 가짜 뉴스(fake news)에 의한 추천인 것으로 밝혀지기도 했다[197]. 구글의 검색 결과가 특정 정당에 더 우호적인 편향성을 드러냈었다는 지적과 함께, 알고리즘이 특정한 정당의 지지에 대해 더욱 편향된 영향을 미칠 수 있을 뿐만 아니라 선거 결과에까지 영향을 준다는 주장은 계속해서 제기되었다. SNS 등의 디지털 수단을 활용한 정보의 제공 프로세스에서 콘텐츠 필터링 알고리즘의 작동을 통해 타겟으로 설정된 사람들에게만 특정 정보를 차별적으로 제공함으로써, 다양한 의사결정을 방해하고 왜곡할 수 있게 된다.

이처럼 알고리즘의 통제 논리는 개발자의 성향이나 세계관에 따라 그 방향이 달라질 수 있게 된다. 알고리즘에 의한 자동화된 의사결정이 제공하는 결과가 전적으로 중립적이라고 볼 수는 없게 되는 것이다. 검색사이트의 검색 결과가 객관성과 공정성을 온전히 담보하지 못함에도 불구하고, 그 결과가 사회에 미치는 영향은 정치, 경제, 문화 등의 모

196) Amit Datta et al(2018)., Discrimination in Online Advertising A Multidisciplinary Inquiry, Proceedings of Machine Learning Research 81, p3.
197) 이원태(2016), p7.

든 분야를 망라하며 이용자 및 시민들의 선호와 판단 그리고 행동까지도 변화하게 만든다. 편향적인 데이터와 이를 통해 학습한 인공지능 알고리즘이 만들어내는 부정적인 결과인 차별, 편견, 배제 등을 효과적으로 규제하고 교정할 수 있는 방안들도 함께 모색되어야 할 필요성이 제기된다[198]. 알고리즘에 기반한 인공지능의 활용이 더욱 급증할 것이라고 예상되는 가운데, 알고리즘이 공정하고 중립적이고 객관적인가에 대한 문제들은 계속해서 논란이 될 것이기 때문이다.

2. GDPR의 프로파일링 및 자동화된 의사결정과 개인정보 주체의 권리

가. 프로파일링 및 자동화된 의사결정의 개념 및 이용 형태

1) 프로파일링 및 자동화된 의사결정의 규범적 개념

‘프로파일링(profiling)’은 자연인에 관한 특정 개인적 요소를 평가하기 위해, 특히 정보주체의 업무 성과, 경제 상황, 건강, 개인 취향 또는 관심사, 신뢰성 또는 행동, 위치 또는 이동을 분석하거나 예측하기 위해 개인정보를 사용하는 모든 형태의 자동화된 개인정보 처리를 의미한다(GDPR 제4조 제4항). 이처럼 일반적으로 프로파일링은 개인이나 개인들의 집단에 대한 정보를 수집하여 이들을 특정 범주나 집단에 포함하기 위해서 그 특성이나 행동 패턴을 분석하고, 이들의 업무 수행 능력, 관심, 가능한 행동을 예측하고 평가하는 처리를 말한다. ‘자동화된 의사결정(automated individual decision-making)’은 개인에 관한 법적 효과를 발생시키거나 개인에게 중요한 영향을 끼치는 사항들을 오직 프로파일링을 포함한 자동화된 처리에 의해서만 결정하는 것을 말한다(GDPR 제22조 제1항).

GDPR의 규율 대상이 되는 프로파일링은 프로파일링 처리가 자동화된 형태이고, 프로파일링 처리가 개인정보에 대해 수행되며, 프로파일링의 목적이 자연인의 개인적 측면을 평가하는 것에 있을 것이 요구된다[199]. 프로파일링은 개인정보의 ‘모든 형태의 자동화

198) 김재완(2019), EU 일반정보보호규정(GDPR)의 알고리즘 자동화 의사결정에 대한 통제로써 설명을 요구할 권리에 대한 쟁점 분석과 전망, 민주법학 제69호, 민주주의법학연구회, pp.284-285.

된 처리(any form of automated processing)’ 라고 규정하므로, 어떤 형태나 방식이라도 자동화된 처리가 이루어지면 인간이 개입된 경우에도 규율 대상인 프로파일링이 된다. 또한, 프로파일링은 자연인의 ‘개인적 측면(personal aspects)’에 대한 평가로서 그에 대한 분석 또는 예측을 목적으로 하는 것이기 때문에, 개인의 나이, 성별, 키 등 개인적인 특성에 기초하여 단순한 평가 또는 분류를 한 경우에도 규율의 대상이 되는 프로파일링이 된다[200].

2) 프로파일링 및 자동화된 의사결정의 이용 형태

프로파일링의 이용 형태에는 ① 일반적 프로파일링, ② 프로파일링에 기초한 의사결정, ③ 프로파일링을 포함한 전적으로 자동화된 의사결정의 세 가지가 있게 된다. 여기에서 ② 프로파일링에 기초한 의사결정과 ③ 프로파일링을 포함한 전적으로 자동화된 의사결정은 다음과 같이 구별된다. 은행 직원이 순전히 자동화된 수단으로 생성된 프로파일에 기초하여 대출 허용 여부를 결정하는 것은 프로파일링에 기초한 의사결정에 해당하는 형태이고, 알고리즘이 대출의 허용 여부를 결정하고 이러한 결정이 자동으로 개인에게 전달되는 것이 프로파일링을 포함한 전적으로 자동화된 의사결정의 형태이다[201]. 이때 ‘자동화된 의사결정’은 다양한 범위를 가지고 있으며 ‘부분적으로’ 프로파일링과 중첩되는 개념이라고 볼 수 있고, ‘전적으로 자동화된 의사결정(solely automated decision-making)’은 인적 개입 없이 기술적인 수단만으로 의사결정을 할 수 있는 역량을 의미하는 것이라고 볼 수 있다[202].

자동화된 의사결정은 설문에 대한 답변과 같이 해당 개인이 직접 제공하는 데이터, 애플리케이션 프로그램을 통하여 수집된 위치정보처럼 개인에 관하여 관찰된 데이터, 신용점수와 같은 이미 생성된 개인적 프로파일로 파생되거나 추정된 데이터 등의 방법에 기초하여서도 이루어질 수 있다[203]. 한편 자동화된 의사결정은 프로파일링과 함께 이루어

199) ARTICLE 29 DATA PROTECTION WORKING PARTY(2018a), Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679(17/EN, WP251, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018. p7.
200) Ibid., p7.
201) Ibid., p8.
202) 이은우 외(2017), 빅데이터 활용과 개인정보보호 균형을 위한 개인정보보호법 개선연구, 국회 행정안전위원회 연구보고서, p64.

질 수도 있고, 단독으로 이루어질 수도 있으며, 마찬가지로 프로파일링도 자동화된 의사결정 없이도 이루어질 수 있다.

프로파일링의 개념 규정에 따라, 프로파일링을 '개인정보를 사용하는 모든 형태의 자동화된 개인정보 처리'라는 점에서 파악할 때, 프로파일링은 자동화된 의사결정의 한 형태가 아니라 '자동화된 처리'의 형태로 파악된다. 한편 GDPR 제22조의 표제가 '프로파일링을 포함한 자동화된 개별적 의사결정(Automated individual decision-making, including profiling)'으로 되어 있어, 마치 프로파일링이 자동화된 의사결정의 한 형태가 되는 것처럼 보이지만, 제4조 제4항과의 관계상 프로파일링은 자동화된 개인정보 처리의 형태이고 이와 함께 자동화된 개별적 의사결정의 형태가 이루어지는 것으로 파악할 수 있다. 컨트롤러는 개인적 프로파일을 이용하여 자동화된 의사결정을 하는 것이므로, 프로파일링은 그 자체로서 자동화된 의사결정이 되지는 못한다. 따라서 GDPR 제22조는 프로파일링을 포함한 자동화된 처리에만 기초한 결정에 따르지 않을 개인정보 주체의 권리를 규정한 것이고, 자동화된 처리인 프로파일링 자체를 제한하는 것은 아니다[204].

나. 프로파일링 및 자동화된 의사결정에 대한 개인정보 처리원칙

1) 적법성, 공정성, 투명성 원칙에 의한 개인정보의 처리

프로파일링 및 자동화된 의사결정에 대한 개인정보 처리는 적법성, 공정성, 투명성의 원칙(lawfulness, fairness and transparency)에 따라야 한다. 프로파일링 및 자동화된 의사결정에 대하여 정보주체에게 간결하고, 투명하며 이해하기 쉽고, 접근하기 쉬운 방식으로 정보를 제공해야 한다. 적법성, 공정성, 투명성의 원칙을 위반하여 공정하지 못한 프로파일링 및 자동화된 의사결정으로 정보주체에게 불이익을 초래해서는 안 된다.

프로파일링 및 자동화된 의사결정에 대한 개인정보의 처리도 목적 제한의 원칙(purpose limitation)에 따라야 한다. 본래의 개인정보를 수집하는 목적 외에 다른 목적으로 프로파일링 및 자동화된 의사결정에 활용할 경우, 별도로 정보주체의 개별적인 동의를 획득하는 등의 추가 조치를 해야만 한다.

---

203) ARTICLE 29 DATA PROTECTION WORKING PARTY(2018a), op. cit., p8.
204) 박노형, 정명현(2018), EU GDPR상 프로파일링 규정의 법적 분석, 안암법학 56권, 안암법학회, p293.

프로파일링 및 자동화된 의사결정에 대한 개인정보 처리는 데이터 최소화 원칙(data minimisation)에 따라야 한다. 프로파일링 및 자동화된 의사결정에 활용되는 개인정보 수집 및 보유 사유를 명확히 입증할 수 있거나 집합(aggregated) 정보 또는 익명처리(anonymised)된 정보를 사용하여 적절한 보호조치를 보장해야 한다.

프로파일링 및 자동화된 의사결정에 대한 개인정보 처리는 정확성 원칙(accuracy)에 따라야 한다. 프로파일링 및 자동화된 의사결정에 사용되는 개인정보가 정확하고 최신의 것인지를 지속해서 검증하는 적절한 방안이 마련되어야 한다.

프로파일링 및 자동화된 의사결정에 대한 개인정보 처리는 보관기간 제한 원칙(storage limitation)에 따라야 한다. 프로파일링 및 자동화된 의사결정에 사용되는 개인정보를 장기간 유지하는 경우, 유출 등에 의한 위험을 초래할 가능성이 크므로 처리 목적에 필요한 단기간의 보관기간을 설정하고 준수해야 한다.

프로파일링 및 자동화된 의사결정에 대한 개인정보 처리는 무결성과 기밀성 원칙(integrity and confidentiality)에 따라야 한다. 프로파일링 및 자동화된 의사결정을 위한 적합한 수학적 또는 통계적 방법을 사용하고, 오류를 시정하고 실수로 인한 위험을 최소화할 수 있는 적절한 기술적·관리적 조치를 시행해야 한다. 또한 차별적인 결과를 방지하기 위하여 정보주체의 이익과 권리에 대한 위험의 크기에 비례하여 개인정보 보호조치를 적용해야 한다.

컨트롤러는 프로파일링 및 자동화된 의사결정에 대한 개인정보 처리원칙이 준수되도록 할 책임이 있으며, 이를 입증할 수도 있어야 한다(제5조 제2항). 컨트롤러는 프로파일링 및 자동화된 의사결정에 대한 개인정보 처리원칙을 엄격히 준수해야 할 책임(accountability)이 있다.

2) 프로파일링 및 자동화된 처리의 합법적 기반인 동의에 관한 원칙

정보주체의 ‘동의(consent)’는 자유롭게 제공된 구체적이며 사전 고지에 입각한 모호하지 않은 정보주체의 의사표시로서, 진술 또는 명확한 긍정의 행위를 통해 자신과 관련한 개인정보 처리에 대한 동의를 표하는 것을 의미한다(제4조 제11항). 여기에서 ‘동의’는 정보주체가 진술 또는 명확한 긍정 행위를 통해 자신에 관한 개인정보의 처리에 승낙을 나타내는 자유로이 주어지고, 구체적이고, 정보에 입각하고, 분명한 의사표시일

것이 요구된다[205].

정보주체에게 프로파일링을 포함해 자동화된 처리만을 바탕으로 한 결정으로서 자신과 관련한 법적 영향 또는 이와 유사하게 중대한 영향을 미치는 결정의 대상이 되지 않을 권리가 인정된다(제22조 제1항). 그러나, 프로파일링을 포함한 자동화된 처리에만 기초한 결정이 정보주체의 명시적 동의에 기초한 경우에는 정보주체에게 자동화된 의사결정의 대상이 되지 않을 권리가 인정되지 않으며, 컨트롤러가 해당 자동화된 개인정보의 처리를 할 수가 있게 된다(제22조 제2항 (c)호).

프로파일링은 정보주체가 직접 제공한 개인정보에 의하기보다 다른 정보에서 추출 또는 추론된 정보에 의존하는 경우가 대부분이다. 이로 인해 프로파일링은 투명하지 않게 이루어질 수 있다. 프로파일링의 합법적 기반으로서 동의에 의존하고자 하는 컨트롤러는 정보주체가 자신이 동의하는 바를 정확히 이해하고 있음을 입증할 필요가 있다. 모든 경우에 정보주체는 자신이 제공하는 동의가 고지에 입각한 선택이 되도록 하기 위해 정보처리의 예상된 용도와 결과에 대해 충분한 관련 정보를 가지고 있어야 한다. 예를 들어, 프로파일링에 대한 동의가 컨트롤러의 서비스 이용을 위한 전제 조건인 상황 또는 고용인과 피고용인의 관계처럼 정보주체에게 선택권이 없는 경우의 동의는 개인정보 처리를 위한 합법적 기반이 될 수가 없다.

다. 프로파일링 및 자동화된 의사결정에 관련된 개인정보 처리 정보를 제공받을 권리

1) 투명성 원칙에 따른 프로파일링 관련 개인정보 처리에 관한 정보의 제공

컨트롤러는 공정하고 투명한 개인정보 처리를 보장하기 위하여 필요한 추가 정보로서 프로파일링을 포함한 자동화된 의사결정의 존재, 그리고 적어도 그러한 경우, 이에 사용되는 로직에 관한 의미 있는 정보와 해당 처리가 정보주체에 대해 갖는 중요성과 예상 결과를 정보주체에게 제공해야 한다(제13조 제2항 (f)호 및 제14조 제2항 (g)호). 이에 의해, 정보주체는 자신에 관하여 법적 효력을 부여하거나 유사하게 중대한 영향을 미치는 프로파일링을 포함하여 자동화된 처리에만 근거한 결정에 따르지 않을 권리를 가진다.

205) ARTICLE 29 DATA PROTECTION WORKING PARTY(2018a), op. cit., p7.

이러한 자동화된 의사결정을 하는 컨트롤러는 첫째 정보주체에게 프로파일링을 포함한 자동화된 의사결정에 관한 개인정보를 처리하고 있음을 알려야 하고, 둘째 관련된 로직에 관하여 의미 있는 정보를 제공하여야 하며, 셋째 해당 개인정보 처리의 중요성과 예상된 결과를 설명해 주어야 한다[206]. 컨트롤러의 개인정보 처리가 제22조 제1항에서 규정한 완전하게 자동화된 의사결정에 해당하지 않는 경우라도, 컨트롤러는 개인정보 처리의 공정성을 위하여 위의 세 가지 정보를 정보주체에게 제공하는 것이 바람직하며, 제13조 및 제14조에 규정된 모든 정보 제공에 대한 요구사항도 준수해야 한다.

GDPR의 기반이 되는 투명성의 원칙을 고려하여 컨트롤러는 프로파일링 또는 자동화된 의사결정 프로세스가 어떻게 기능하는지에 대해 명확하고 간략하게 설명해야 한다. 특히 제22조에 해당하는 것인지 여부와 관계없이, 개인정보처리가 프로파일링 기반의 의사결정을 수반하는 경우, 프로파일링 및 프로파일링 기반의 의사결정을 위해 개인정보처리가 수행된다는 사실이 정보주체에게 명확히 통지되어야 한다. 정보주체는 컨트롤러로부터 개인정보 처리에 관한 정보를 제공받을 권리(통지를 받을 권리), 그리고 특정한 상황에서는 수행된 프로파일링을 기반으로 한 완전히 자동화된 개인 의사결정 여부와 관계없이 '프로파일링'에 대한 거부할 권리(반대권)가 있다[207].

2) 관련된 로직에 관한 의미 있는 정보의 제공

머신 러닝의 성장과 복잡성은 자동화된 의사결정 프로세스와 프로파일링이 어떻게 이루어지는지에 대해 이해하는 것을 어렵게 만들 수 있다. 컨트롤러는 사용된 알고리즘에 대한 복잡한 설명 또는 전체 알고리즘에 대한 공개를 시도할 필요 없이, 그에 대한 근거 또는 결정에 도달하기 위해 사용된 기준에 대해 정보주체에게 간단하게 설명할 수 있는 방법을 찾아야 하며, 이때 제공된 정보는 정보주체에게 의미 있는 것이어야 한다[208]. 예를 들어, 컨트롤러가 신용점수를 이용하여 개인의 대출 신청을 평가하고 거부하는 경우를 보자. 신용점수는 신용 조회 기관이 제공했거나 컨트롤러가 보유한 정보를 기반으로 계산한 것일 수 있다. 정보의 출처와 관계없이(정보주체로부터 정보를 수집한 것이 아닌 경우에는 제14조 제2항 (f)호에 따라 정보 출처에 대한 정보를 정보주체에게 제공해야

206) Ibid., p18.
207) Ibid., p34.
208) Ibid., p19.

함), 컨트롤러가 이 점수에 의존하는 경우, 컨트롤러는 정보주체에게 이러한 사실과 그 근거에 대해 설명할 수 있어야 한다. 컨트롤러는 이 프로세스가 공정하고 책임 있는 대출 결정을 내리는 데 도움을 준다고 설명한다. 컨트롤러는 결정을 내리는 데 고려한 주요 특징들, 정보의 출처, 그리고 적절성에 대한 세부 사항을 제공한다. 여기에는 신청서 작성 시 정보주체가 제공한 정보, 체납금을 포함한 이전 계정 활동에 대한 정보, 사기 기록 정보 및 파산 기록과 같은 공식적인 공공 기록 정보와 같은 것들이 포함될 수 있다. 또한 컨트롤러는 사용된 신용점수 산정 방식이 공정하고, 효과적이며, 공평한지에 대해 정기적으로 시험이 수행되었다는 사실을 정보주체에게 통지한다. 컨트롤러는 제22조 제3항에 따라 정보주체가 거부 결정에 대해 재심사를 요구할 수 있는 연락 정보를 제공한다.

특히 복잡성은 정보주체에게 정보를 제공하지 못하는 이유가 될 수 없다. 투명성의 원칙에 따라, 대중이나 정보주체에게 전달되는 모든 정보는 간결하고 쉽게 접근할 수 있으며 이해하기 쉬워야 하고, 명확하고 평이한 표현을 사용해야 하며, 적절한 경우 추가적 시각 자료를 사용해야 한다. 해당 정보는 전자적 형태로, 예를 들어 대중에 전달될 때 웹사이트를 통해 제공될 수 있다. 이는 온라인 광고의 경우에서처럼, 행위자의 급증과 업무의 기술적 복잡성 때문에 정보주체 입장에서 자신의 개인정보가 수집되고 있는지 여부와 누가 무슨 목적으로 개인정보를 수집하는지를 인지하고 이해하기 어려운 상황과 특히 관련이 있다(전문 58).

3) 해당 개인정보 처리의 중요성과 예상된 결과의 설명

컨트롤러는 정보주체에게 해당 개인정보 처리의 중대성과 예상된 결과를 설명하여야 한다. 정보주체에게 제공되어야 할 정보는 계획되거나 향후의 개인정보 처리에 대한 사항들, 그리고 자동화된 의사결정이 어떻게 정보주체에게 영향을 미칠 것인가 하는 것에 대한 사항들이어야 한다. 정보주체는 특히 프로파일링을 포함한 자동화된 의사결정 알고리즘의 사용이 수반된 경우, 정보처리의 근본이 되는 추론과 그 결과에 대해 알 권리가 있다. 예를 들어 신용점수의 경우, 정보주체는 결정 자체에 대한 정보뿐 아니라 자신의 정보처리 및 ‘yes’ 또는 ‘no’ 결정의 근거 논리를 알 권리가 있다. 이러한 요소들에 대한 이해가 없이는 거부할 권리와 관할 기관에 대한 민원을 제기할 권리와 같은 기타

필수적인 안전 대책들을 효과적으로 행사할 수 없다[209].

개인정보 처리의 중대성과 예상된 결과를 설명해야 하는 정보가 의미 있고 이해 가능한 것이 되도록 하기 위해서는 가능한 효과의 종류에 대한 실제적이고 구체적인 예가 제시되어야 한다. 예를 들어, 한 보험회사에서 대상 고객의 운전 행동을 기반으로 자동차 보험료를 결정하기 위한 자동화된 의사결정 프로세스를 사용하는 경우가 있다. 이때 회사는 해당 개인정보 처리의 중요성과 예상되는 결과를 보여주기 위해서 위험한 운전이 높은 보험료로 이어질 수 있다는 점을 설명하고, 급가속과 급제동과 같은 위험한 운전 습관과의 비교를 포함하여 가공의 운전자들을 비교하는 앱을 제공하며, 한편 그래픽을 이용하여 운전 습관을 개선하고 보험료를 낮출 수 있는 팁도 제공할 수 있다[210].

라. 프로파일링을 포함한 자동화된 의사결정에 대한 정보에의 접근권

정보주체는 프로파일링을 포함한 자동화된 의사결정에 대하여 그 정보에 대해 접근할 수 있는 권리를 가진다(제13조 제2항 (f)호와 제14조 제2항 (g)호의 요구와 동일한 접근권). 이에 따라, 정보주체는 프로파일링을 포함하는 자동화된 의사결정의 존재, 자동화된 의사결정에 활용된 로직에 대한 의미 있는 정보, 정보주체에 대한 해당 개인정보 처리의 중요성과 예상되는 결과에 대해 접근할 수 있는 권리를 가진다(제15조 제1항 (h)호). 이것은 정보주체가 프로파일 작성에 사용된 정보의 범주를 포함하여 프로파일링에 사용된 개인정보의 내용을 확인할 수 있는 권리를 규정한다.

정보주체는 정보처리의 합법성을 인지하고 확인하기 위해, 자신에 대해 수집된 개인정보에 접근할 수 있는 권리와 해당 권리를 합리적 간격으로 쉽게 행사할 수 있는 권리를 가져야 한다. 여기에는 정보주체가 자신의 건강 관련 정보, 예를 들어 담당 의사의 진단, 검사 결과, 평가와 제공된 치료법 및 중재술 등의 정보를 담고 있는 의료기록정보에 접근할 수 있는 권리가 포함된다. 이에 따라 모든 정보주체는 특히 개인정보 처리 목적, 가능한 경우 개인정보 처리 기간, 개인정보 수령자, 개인정보 자동처리에 사용되는 로직, 그리고, 적어도 프로파일링에 기초한 경우, 해당 처리의 결과에 대해 알고 이에 대한 알림(통지)을 받을 권리가 있다. 가능한 경우, 컨트롤러는 정보주체가 자신의 개인정보에

209) Ibid., p20.
210) Ibid., pp20-21.

직접 접근할 수 있도록 하는 보안 시스템에 대한 원격 접근권을 제공할 수 있어야 한다. 한편, 그러한 권리는 영업비밀이나 지적재산권, 그리고 특히 소프트웨어를 보호하는 저작권을 포함한 타인의 권리나 자유에 악영향을 미쳐서는 안 된다. 하지만 이를 고려한 결과가 정보주체에 대해 모든 정보 제공을 거절하는 것이 되어서는 안 된다. 컨트롤러가 정보주체와 관련한 정보를 대량으로 처리하는 경우, 컨트롤러는 해당 정보를 전달하기 전에 정보주체에게 요청 대상 정보 또는 관련 처리 활동을 명시해 달라고 요청할 수 있어야 한다(전문 63).

마. 부정확한 개인정보에 기반한 프로파일링 및 자동화된 의사결정에 대한 수정권

프로파일링 및 자동화된 의사결정은 부정확성의 위험을 높여주는 예측의 요소를 포함할 수 있다. 입력 정보가 부정확하거나 관련성이 없거나, 또는 맥락에서 벗어난 것일 수 있다. 상관관계를 파악하기 위해 사용되는 알고리즘에 문제가 있을 수도 있다. 이에 따라 정보주체는 자신에 관한 부정확한 개인정보를 수정하고, 추가 진술의 제공을 통해 불완전한 개인정보를 보완할 권리가 있다(제16조). 이러한 수정권은 예를 들어, 개인이 업무수행 능력에 대한 사항을 보여주는 범주로 분류되고, 이러한 프로파일링이 잘못된 정보를 기반으로 한 경우에 적용될 수 있다. 정보주체는 사용된 정보, 그리고 자신에게 적용된 그룹 또는 범주의 부정확성에 대해 이의를 제기하고 수정을 요구할 수 있다[211].

또한 정보주체가 추가 정보를 이용하여 프로파일링 및 자동화된 의사결정에 사용된 불완전한 개인정보를 보완할 수 있는 권리도 인정된다. 구체적인 예로, 한 지방 병원의 컴퓨터 시스템에서 어느 환자를 심장병 위험이 높은 그룹으로 분류했다고 가정해 보자. 비록 환자가 심장병을 앓고 있지 않더라도 이 '프로파일'이 반드시 부정확한 것은 아니고, 이 프로파일은 해당 개인이 심장병을 앓을 확률이 높다고 명시하고 있을 뿐이다. 이는 통계학적으로 실제에 가까울 수 있다. 그럼에도 불구하고 정보주체는 정보처리의 목적을 고려하여 보충 사항을 제공할 권리가 있다. 이는 제한된 기능을 가진 현지 병원의 시스템보다 세밀한 검사와 추가 정보의 분류가 가능한 첨단 의료 컴퓨터 시스템 및

211) Ibid., p35.

통계 모델을 기반으로 이루어질 수 있다[212].

이러한 수정권은 프로파일링 및 자동화된 의사결정 생성에 사용된 정보주체의 개인정보인 '입력 정보' 및 해당 정보주체와 관련된 개인정보인 프로파일 자체 또는 정보주체에 대해 매겨진 점수인 '출력 정보'에 대해 모두 적용된다.

바. 프로파일링 등에 관련된 개인정보의 삭제권(잊힐 권리)

정보주체는 자신에 관한 개인정보를 부당한 지체 없이 삭제하도록 컨트롤러에게 요청할 권리를 가진다. 컨트롤러는 정보주체가 프로파일링 등 본인과 관련한 개인정보의 처리를 거부하고 이보다 우선하는 처리의 정당한 근거가 없는 경우, 또는 정보주체가 직접 마케팅을 목적으로 한 프로파일링 처리를 거부한 경우, 부당한 지체 없이 개인정보를 삭제할 의무가 있다(제17조 제1항 (c)호).

삭제권은 프로파일링 등에 사용된 입력 정보와 출력 정보 모두에 적용된다. 동의를 기반으로 프로파일링이 이루어지고 이러한 동의가 철회된 경우, 컨트롤러는 프로파일링에 대해 또 다른 법적 근거가 있는 경우를 제외하고 관련 개인정보를 삭제해야 한다.

사. 프로파일링 등에 관련된 개인정보의 처리에 대한 제한권

정보주체는 컨트롤러의 정당한 이익이 정보주체의 정당한 이익보다 더 우선하는 여부를 확인할 때까지, 정보주체가 프로파일링 등 본인과 관련한 개인정보의 처리에 대해 거부하는 경우, 컨트롤러의 처리를 제한할 권리를 가진다(제18조 제1항 (d)호).

이처럼 개인정보의 처리가 제한되는 경우, 그 개인정보는 보관을 제외하고, 정보주체의 동의가 있거나 법적 권리의 확립이나 행사 및 방어를 위해, 또는 제3자나 법인의 권리를 보호하거나 유럽연합 또는 회원국의 중요한 공익상의 이유에 한해서만 처리될 수 있다(제18조 제2항). 처리의 제한권을 가진 정보주체는 처리 제한권이 해제되기 전에 컨트롤러로부터 이를 고지받아야 한다(제18조 제3항).

이러한 개인정보의 처리를 제한할 권리는 프로파일링 과정의 모든 단계에 적용된다. 따라서 정보주체가 컨트롤러의 개인정보 처리에 대한 제한권을 가지게 되는 경우, 프로

212) Ibid., pp35-36.

파일링을 포함한 자동화된 의사결정 과정의 모든 단계에 해당 개인정보 처리를 차단하거나 제한할 권리가 적용된다.

아. 프로파일링을 포함한 개인정보 처리에 대한 정보주체의 거부권(반대권)

정보주체는 자신의 특별한 상황에 따라 공익이나 컨트롤러의 공식 권한 행사로 이루어지는 업무수행에 처리가 필요한 경우 및 컨트롤러 또는 제3자의 정당한 이익 목적을 위해 처리가 필요한 경우에 근거한 프로파일링 등, 자신과 관련한 개인정보의 처리에 대해 언제든지 거부(반대)할 권리를 가진다. 컨트롤러는 정보주체의 이익, 권리 및 자유보다 더 우선하는 처리를 위한 또는 법적 권리의 확립, 행사나 방어를 위한 설득력 있는 정당한 이익을 증명하지 못하는 한, 해당 개인정보를 더 이상 처리해서는 안 된다(제21조 제1항).

직접 마케팅을 목적으로 개인정보가 처리되는 경우, 정보주체는 언제든지 해당 직접 마케팅과 관련한 프로파일링을 포함하여, 그러한 마케팅을 위한 자신에 관한 개인정보 처리를 거부할 권리를 가진다(제21조 제2항). 정보주체가 직접 마케팅 목적을 위한 처리를 거부하는 경우, 컨트롤러는 더 이상 그러한 목적으로 개인정보를 처리해서는 안 된다(제21조 제3항).

이러한 프로파일링을 포함한 개인정보 처리에 대한 정보주체의 거부권은 아무리 늦어도 정보주체에게 처음 고지한 시점에, 명백하게 정보주체에게 통지되어야 하며, 정보주체의 주의를 확실하게 끌 수 있도록 다른 정보와는 별도로 명확하게 제시되어야 한다(제21조 제4항). 정보사회 서비스 사용과 관련하여(지침 2002/58/EC와 관계없이), 정보주체는 기술 사양서(technical specifications)를 사용하는 자동화된 수단을 통해 거부권을 행사할 수 있다(제21조 제5항).

개인정보가 과학적 또는 역사적 연구 목적이나 통계적 목적을 위해 처리되는 경우로서, 공익을 위한 업무수행에 필요한 처리가 아니라면, 정보주체는 자신의 특정 상황과 관련한 근거를 바탕으로 자신에 관한 개인정보 처리를 거부할 권리를 가진다(제21조 제6항).

정보주체가 거부권을 행사하면, 컨트롤러는 정보주체의 권리와 자유보다 더 중대한 부

득이한 적법한 근거를 증명할 수 있는 경우를 제외하고 처리작업을 중단하거나 개시하지 않아야 하며, 관련 개인정보를 삭제해야 할 경우도 있게 된다. 이때 부득이한 적법한 근거가 되는 내용에 대해서는 GDPR에서 명시하고 있지 않다. 과학연구의 수행이나 전염병의 확산을 예측하기 위한 프로파일링 등이 컨트롤러의 사업상 이익뿐 아니라 사회 전반에 이익이 되는 경우라면, 이를 부득이한 적법한 근거가 될 수 있는 경우라고 할 수 있다.

또한 컨트롤러는 프로파일링이 정보주체에게 미치는 영향이 특정한 목적을 충족하기 위한 최소 필요 사항으로 제한된다는 점을 증명할 필요가 있다. 즉, 프로파일링이 해당 목적상 조직에 매우 중요한 것이고, 이를 달성하기 위해 최소의 침해를 발생시키는 방법으로 행하여져야 한다. 이것은 컨트롤러의 이익과 정보주체의 거부권의 제기 근거(개인적, 사회적 또는 직업적 이유 등) 사이에서 항상 균형이 이루어져야 한다는 것을 의미한다. 이와 같은 모든 부득이한 적법한 근거의 증명책임은 정보주체가 아닌 컨트롤러에게 있다.

직접 마케팅과 관련된 범위까지의 프로파일링을 포함하여, 정보주체가 직접 마케팅 목적의 개인정보 처리에 이의를 제기할 수 있는 무조건적인 권리가 정보주체에게 제공된다(제21조 제2항, 제3항). 이것은 컨트롤러의 이익과 정보주체 사이의 이익의 균형을 고려할 필요가 없다는 것을 의미한다. 즉, 컨트롤러는 정보주체의 이의제기의 이유를 묻지 않고 정보주체의 의사를 존중해야만 한다.

또한 직접 마케팅을 목적으로 개인정보가 처리되는 경우, 정보주체는 최초 처리 또는 추가 처리와 관련 있는지 여부와 상관없이, 해당 직접 마케팅과 관련한 프로파일링을 포함하여 그러한 처리를 거부할 수 있는 권리를 언제든지 무상으로 가져야 한다. 이 권리는 정보주체가 명백하게 인지할 수 있도록 제공되어야 하며 다른 기타 정보와는 별도로 명백하게 제시되어야 한다(전문 70).

자. 정보주체의 프로파일링 및 자동화된 의사결정의 대상이 되지 않을 권리

1) 권리의 적용원칙

온라인 신용거래 신청 자동 거절이나 인간의 개입이 없는 전자 채용 절차 등과 같이,

자동화된 처리만을 바탕으로 정보주체의 개인적 요소를 평가하는 조치를 포함하여, 정보주체는 자신과 관련한 법적 영향 또는 이와 유사하게 중대한 영향을 미치는 결정의 대상이 되지 않을 권리를 가진다(전문 71). 이에 따라, 정보주체는 프로파일링을 포함해 자동화된 처리만을 바탕으로 한 결정으로서 자신과 관련한 법적 영향 또는 이와 유사하게 중대한 영향을 미치는 결정의 대상이 되지 않을 권리를 가진다(제22조 제1항).

여기에서 자동화된 처리만을 바탕으로 한 결정이란 의사결정 과정에 사람이 관여하지 않는 것을 의미한다. 컨트롤러가 인간의 참여를 조작하여 제22조의 적용을 회피할 수는 없다. 예를 들어, 누군가 실제 결과에 영향을 주지 않고 자동으로 생성된 프로파일을 개인에게 적용하는 경우, 이것은 여전히 자동화된 처리에만 기반한 결정이 되어 제22조의 적용을 받게 된다[213]. 인간의 개입으로 인정되기 위해서는, 컨트롤러가 그 결정에 대한 인간의 검토가 단순히 형식적인 제스처가 아니라 의미가 있는 것으로 보장해 주어야만 하고, 그 결정을 변경할 권한과 능력이 있는 사람에 의해서 수행되어야 하며, 분석의 일부로서 활용 가능한 모든 입력 및 출력 정보도 고려해야 한다[214].

GDPR은 '법적 영향(legal effects)'과 '유사하게 중대한 영향을 미치는(similarly significantly affects)' 것이 어떤 것인지에 대해서는 구체적으로 명시하고 있지는 않다. 먼저 법적 영향이란 개인의 법적 권리나 지위 또는 계약상 권리에 부정적인 영향을 주는 것을 의미하는 것으로 볼 수 있으며, 이때 법적 권리는 결사의 자유, 선거권 또는 법적 조치를 할 수 있는 권리 등을 말하는 것으로 볼 수 있다. 법적 권리나 지위 또는 계약상 권리에 부정적인 영향을 주는 것으로는 어떤 사람에게 육아나 주택 수당과 같이 법으로 주어지는 사회보장 혜택이 거부되는 경우, 입국이 거부되는 경우, 소관 당국에 의한 보다 엄격한 보안 조치 또는 감청의 집행, 휴가를 가기 전에 요금을 지불하는 것을 잊었고 이 때문에 계약 위반으로 처리되어 휴대폰 서비스가 자동으로 연결이 끊어지게 된 경우 등을 들 수 있다[215].

다음으로 의사결정 과정이 사람들의 법적 권리에 영향을 미치지는 않더라도, 그것이 동등하거나 유사하게 영향을 미치는 경우 제22조의 범위에 속할 수 있게 된다. 법적 권리 또는 의무에 특별히 영향을 주지 않는 경우라도 정보주체에게 제22조에 따른 보호를

213) Ibid., p10.
214) Ibid., p10.
215) Ibid., p10.

요구할 정도로 중대한 영향을 주는 경우도 있을 수 있다는 것을 의미한다. 개인정보의 처리가 어떤 사람에게 중대하게 영향을 미치려면 그 처리의 영향이 사소한 것 이상이어야 하며, 주의를 기울일 만큼 충분히 크거나 중요해야 한다. 즉, 결정은 해당 개인의 상황, 행동 또는 선택에 중대하게 영향을 줄 수 있는 잠재력을 가져야 한다. 가장 극단적인 결정의 경우에는 개인의 배제 또는 차별로 이어질 수 있게 된다. 자동화된 의사결정으로 차등적 가격이 부과되는 경우, 특정 상품이나 서비스를 구매할 수 없도록 극심하게 높은 가격을 요구하는 것은 중대한 영향이라고 볼 수 있다[216]. 이때, 유사하게 중대한 영향은 긍정적일 수도 있고 부정적일 수도 있으며, 이러한 영향은 해당 자동화된 결정에 관계되는 사람이 아닌 다른 사람의 행위로 발생할 수도 있게 된다.

프로파일링 및 자동화된 의사결정의 대상이 되지 않을 권리는 일반적으로 자동화된 의사결정에 반대할 권리로도 해석된다. 실제에 있어서 정보주체에게 법적 효력을 발생시키거나 이와 유사하게 중대한 영향을 주는 프로파일링 및 자동화된 의사결정에 해당 정보주체의 동의가 필요할 것이다.

2) 프로파일링을 포함한 완전하게 자동화된 의사결정이 허용되는 경우

자동화된 의사결정이 정보주체와 컨트롤러 사이의 계약 체결 또는 이행에 필요한 경우, 컨트롤러가 준수해야 하며 정보주체의 권리 및 자유와 정당한 이익을 보호하기 위한 적절한 조치를 규정하는 유럽연합이나 회원국 법률이 허가하는 경우, 정보주체의 명시적 동의에 기초한 경우에는 프로파일링을 포함한 자동화된 처리 결정의 대상이 되지 않을 권리가 적용되지 않는다(제22조 제2항). 이에 의해, 프로파일링을 포함한 자동화된 처리에만 기초한 결정이 위의 세 가지 경우 중의 어느 하나에 해당하면, 정보주체에게 자동화된 의사결정의 대상이 되지 않을 권리가 인정되지 않으며, 컨트롤러가 해당 자동화된 개인정보의 처리를 할 수가 있게 된다.

정보주체와 컨트롤러 사이에 계약을 체결하거나 이행하기 위하여 '필요한(necessary)' 경우에, 법적 효력을 부여하거나 유사하게 중대한 영향을 미치는 프로파일링을 포함하여 완전하게 자동화된 의사결정은 금지되지 않는다. 인간의 오류, 차별 및

216) Ibid., p11.

권한 남용 등의 가능성을 낮추는 등 의사결정 과정에서 일관성 또는 공정성을 높이거나, 신용 조회를 통하여 상품이나 서비스에 대한 비용을 지불하지 못하는 고객의 위험을 감소시키거나, 고객에게 보다 짧은 시간 내에 결정을 내리게 하거나 그 과정의 효율성을 증대시키는 경우 등이 해당한다[217].

하지만, 그러한 예외의 근거로서 '필요한(necessary)'의 의미는 좁게 해석되어야 한다. 컨트롤러는 프로파일링이 필요하다고 증명할 수 있어야 하는데, 해당 프로파일링보다 프라이버시가 덜 침해되는 수단이 채택될 수 있는지도 고려되어야 하므로, 같은 목적을 달성하는 '다른 덜 침해적인 수단(other less intrusive means)'이 존재한다면, 해당 프로파일링은 필요하지 않게 될 것이다[218].

컨트롤러가 준수해야 하며 정보주체의 권리 및 자유와 정당한 이익을 보호하기 위한 적절한 조치를 규정하는 유럽연합이나 회원국 법률이 자동화된 의사결정을 허가하는 경우에는, 법적 영향을 발생시키거나 이와 유사하게 중대한 영향을 미치는 프로파일링을 포함한 완전하게 자동화된 의사결정은 금지되지 않고 허용된다. 여기에는 유럽연합 기관 또는 국가 감독기관의 규정, 표준, 권고에 따라 수행되는 사기 및 세금 회피 모니터링 및 방지 목적을 위한 경우, 컨트롤러가 제공하는 서비스의 보안과 신뢰성을 확보하기 위한 경우가 해당한다(전문 71). 유럽연합 또는 회원국의 법률로 부과될 수 있는 프로파일링에 기초한 결정에 대한 제한은, 공공안전 등을 보호하기 위하여 민주사회에서 필요한 경우에 비례적으로 부과될 수도 있다(전문 73).

정보주체의 명시적 동의에 근거한 경우에는 법적 영향을 부여하거나 유사하게 중대한 영향을 미치는 프로파일링을 포함한 완전하게 자동화된 의사결정이 금지되지 않는다. 정보주체에게 법적 영향을 부여하거나 유사하게 중대한 영향을 미치는 프로파일링을 포함한 자동화된 의사결정은 정보주체에게 개인정보 보호에 대하여 상당한 위험을 발생시킨다는 점에서, 정보주체는 자신의 개인정보에 대하여 높은 수준의 통제에 해당하는 명시적 동의를 하는 것이다. GDPR에서 '명시적 동의(explicit consent)'에 대해 구체적인 개념 정의를 두고 있지는 않지만, 명시적 동의란 '적극적 행위(affirmative action)'가 아닌 '명백한 진술(express statement)'로서 그 내용이 구체적으로 확인되어야 하는 것으

217) Ibid., p12.
218) Ibid., pp12-13.

로 보아야 한다[219].

3) 정보주체를 보호하기 위한 적절한 조치의 이행 의무

프로파일링을 포함한 완전하게 자동화된 의사결정이 허용되는 예외적 경우에 해당하는 경우, 컨트롤러는 정보주체의 권리 및 자유와 정당한 이익으로서 최소한 컨트롤러 측의 인간의 개입을 받을 권리, 자신의 견해를 표현할 권리, 결정에 이의를 제기할 권리를 보호하기 위한 적절한 조치를 이행해야 한다(제22조 제3항).

이때 특히 중요한 부분은 '인간의 개입(human intervention)'이다. 그런데 문제는 이러한 인간의 개입이 어떻게 이루어져야 하는지가 불분명하다는 것이다. 인간의 개입이 이루어지기 위해서는, 컨트롤러가 그 결정에 대한 인간의 검토가 단순히 형식적인 제스처가 아니라 의미가 있도록 보장해 주어야만 하고, 또한 이러한 개입의 주체 또는 평가자는 그 결정을 변경할 수 있는 권한도 가져야 한다. 이를 위하여 정보주체가 제공하는 추가적 정보를 포함한 모든 관련 정보에 대한 철저한 평가도 요구된다[220].

정보주체와 관련한 공정하고 투명한 정보처리를 보장하기 위해, 개인정보가 처리되는 구체적 상황과 맥락을 고려하여, 컨트롤러는 프로파일링을 위한 적절한 수학 또는 통계 절차를 사용하고, 적절한 기술적, 조직적 조치를 이행하여 특히 개인정보의 부정확성을 일으키는 요인을 시정하고 오류 위험을 최소화하며, 정보주체의 이익 및 권리를 위해 관련된 잠재 위험을 고려하고 특히 출신 인종 또는 민족, 정치적 견해, 종교 또는 신념, 노동조합 가입 여부, 유전 또는 건강 상태, 또는 성적 지향 등에 기초한 정보주체에 대한 차별적 영향을 방지하거나 그러한 효과를 지닌 조치가 이루어질 수 있는 방식으로 개인정보를 안전하게 관리해야 하며, 특수한 범주의 개인정보에 기초한 자동화된 의사결정 및 프로파일링은 특정 조건에서만 허용되어야 한다(전문 71). 이와 같은 정보주체를 보호하기 위한 적절한 조치는 개인정보 처리의 설계 단계에서부터 계속해서 지속적으로 이루어져야만 한다.

원칙적으로 특수한 범주의 개인정보 처리(Processing of special categories of personal data)는 금지된다. 출신 인종 또는 민족, 정치적 견해, 종교 또는 철학적 신념, 노동조합

219) Ibid., pp12-13.
220) Ibid., p16.

가입 여부를 드러내는 개인정보의 처리, 그리고 유전정보, 자연인의 고유 식별을 목적으로 한 생체정보, 건강 관련 정보나 자연인의 성생활 또는 성적 지향과 관련한 정보의 처리는 금지된다(제9조 제1항). 하지만 정보주체가 하나 이상의 구체적 목적을 위한 개인정보 처리에 명시적으로 동의한 경우(제9조 제2항 (a)호), 또는 그 추구하는 목적에 비례하고 개인정보 보호에 대한 권리의 본질을 존중하며, 정보주체의 기본권과 이익을 보호하기 위한 적절하고 구체적인 조치를 규정하는 유럽연합이나 회원국 법률을 바탕으로 하여 상당한 공익을 이유로 처리가 필요한 경우(제9조 제2항 (g)호)에는 특수한 범주의 개인정보 처리가 금지되지 않는다. 한편 정보주체가 하나 이상의 구체적 목적을 위한 개인정보 처리에 명시적으로 동의한 경우라도, 유럽연합 또는 회원국의 법률이 특수한 범주의 개인정보 처리의 금지 규정을 정보주체가 해제하지 못한다고 규정하는 경우는 허용되지 않고 여전히 금지된다(제9조 제2항 (a)호 단서).

프로파일링을 포함한 완전하게 자동화된 의사결정이 허용되어 컨트롤러가 해당 자동화된 개인정보를 처리할 수 있는 예외적 경우(제22조 제2항)에는, 정보주체의 명시적 동의(제9조 제2항 (a)호) 또는 법률에 기초한 상당한 공익상 이유(제9조 제2항 (g)호)가 적용되어 특수한 범주의 개인정보 처리가 허용된다(제22조 제4항). 하지만, 정보주체의 권리 및 자유와 정당한 이익을 보호하기 위한 적절한 조치가 존재하는 경우가 아니라면, 특수한 범주의 개인정보에 기초해서 해당 자동화된 개인정보를 처리해서는 안 된다(제22조 제4항).

3. 우리나라 신용정보법의 자동화평가에 대한 정보주체의 권리

신용정보법은 개인신용정보주체에게 자동화평가 결과에 대한 설명 및 이의제기권을 보장하고 있다(제36조의2). 개인인 신용정보주체는 개인신용평가회사 등에 대하여 개인신용평가, 대통령령으로 정하는 금융거래의 설정 및 유지 여부, 내용의 결정(대통령령으로 정하는 신용정보제공·이용자에 한정), 그 밖에 컴퓨터 등 정보처리장치로만 처리하면 개인신용정보 보호를 저해할 우려가 있는 경우로서 대통령령으로 정하는 행위에 자동화평가를 하는지 여부의 사항을 설명하여 줄 것을 요구할 수 있다(제36조의2 제1항 제1호). 또한 자동화평가를 하는 경우에는 자동화평가의 결과, 자동화평가의 주요 기준, 자동화

평가에 이용된 기초정보의 개요, 그 밖에 이러한 사항과 유사한 사항으로서 대통령령으로 정하는 사항에 대하여 설명하여 줄 것을 요구할 수 있다(제36조의2 제1항 제2호).

개인신용정보주체는 개인신용평가회사 등에 대하여 해당 신용정보주체에게 자동화평가 결과의 산출에 유리하다고 판단되는 정보의 제출을 하게 할 수 있다(제36조의2 제2항 제1호). 또한 자동화평가에 이용된 기초정보의 내용이 정확하지 아니하거나 최신의 정보가 아니라고 판단되는 경우 기초정보를 정정하거나 삭제할 것을 요구하는 행위, 자동화평가 결과를 다시 산출할 것을 요구하는 행위를 할 수 있다(제36조의2 제2항 제2호). 이에 대해 개인신용평가회사 등은 신용정보법 또는 다른 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, 해당 신용정보주체의 요구에 따르게 되면 금융거래 등 상거래관계의 설정 및 유지 등이 곤란한 경우, 그 밖에 그러한 경우들과 유사한 경우로서 대통령령으로 정하는 경우의 어느 하나에 해당하는 경우에는 제1항 및 제2항에 따른 개인신용정보주체의 요구를 거절할 수 있다(제36조의2 제3항).

4. 개선방안

우리나라의 개인정보 보호 법제에서 프로파일링 및 자동화된 의사결정에 대한 직접적인 정의 규정은 마련되어 있지 않다. 개인정보 보호법에서는 ‘처리’란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 말하는 것으로 정의하고 있다(제2조 제2호). 신용정보의 이용 및 보호에 관한 법률(신용정보법)에서는 ‘처리’란 신용정보의 수집(조사를 포함), 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 결합, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 말하는 것으로 정의하고(제2조 제13호), ‘자동화평가’란 신용정보회사 등의 종사자가 평가 업무에 관여하지 아니하고 컴퓨터 등 정보처리장치로만 개인신용정보 및 그 밖의 정보를 처리하여 개인인 신용정보주체를 평가하는 행위를 말하는 것으로 정의한다(제2조 제14호).

개인정보 보호법에서는 프로파일링 및 자동화된 의사결정에 관한 규정은 전혀 없으며, 신용정보법은 신용정보와 관련해서만 부분적으로 자동화평가를 규정하고 있을 뿐이다. 신용정보법은 자동화평가는 기본적으로 가능하고 단지 자동화평가와 관련된 설명을 요구

하고 추가 정보를 제공할 권리만을 인정하고 있다. 이에 인적개입을 요구할 권리의 여지는 볼 수가 없다. 또한 신용정보주체의 자동화된 평가가 모두 GDPR 제22조의 의미에서 '법적 영향을 발생시키거나 이와 유사하게 중대한 영향을 미치는 자동화된 처리' 인지, 아니면 GDPR보다 폭넓게 규제하고자 하는 것인지는 모호하다. 더욱 큰 문제는 처음부터 신용평가 자체가 정보주체의 동의 없이 이루어지고 있다는 점이다. 마찬가지로 신용정보법은 정보주체의 권리에 대해 사전에 정보주체에게 고지할 의무를 포함하고 있지도 않다.

개인정보의 보호를 위한 일반법이자 기본법이라고 할 수 있는 개인정보 보호법에서 인공지능시스템으로 인한 개인정보 침해 문제를 규율할 수 있는 기초적인 규범조차 마련되어 있지 않은 것은 커다란 문제라고 생각한다. 우리나라의 개인정보 보호 법제에서 프로파일링 및 자동화된 의사결정에 대한 직접적인 규정이 마련되어 있지 않기 때문에, 이에 대한 정보주체의 권리 인정 및 감독기관의 감독규제에 한계와 공백을 초래하게 될 것이다.

따라서 GDPR의 프로파일링 및 자동화된 의사결정에 관한 개념 및 정보주체의 권리 규정을 참조하여 우리나라 개인정보 보호 법제에 마련해야 할 것으로 보인다.

제5절 동의제도 개선 방안

개정 개인정보 보호법의 핵심 취지 중의 하나는 신산업 육성을 위한 데이터 이용 활성화를 지원하기 위해 정보주체의 동의 없이 과학적 연구, 통계 작성 등의 목적으로 가명정보를 이용할 수 있는 근거를 마련한 것이다. 한편 이와 별개로 현행 동의 제도가 지나치게 복잡하고 현실성이 없다고 비판하며 개선해야 한다는 주장이 인터넷 기업들을 중심으로 제기되어 왔다. 한국인터넷기업협회는 지난 2019년 9월, <역차별 해소를 위한 개인정보 동의제도 개선의 필요성>이라는 행사[221]를 개최하였으며, 인터넷 사업자들은 2020년 국회 국정감사 당시에도 '인터넷 서비스 동의제도 개선 필요성 및 개선 방향' 이란 제목의 설명자료를 만들어 의원실에 배포했다고 한다[222].

221) 인터넷기업협회, 2019.9.26., <http://kinternet.org/club/view/420>.
222) 한겨레, 2020.10.19., 개인정보 보호막 '동의 절차'…업계 입김에 '흔들', <http://www.hani.co.kr/arti/science/technology/966260.html>.

개인정보 보호위원회가 발간한 <2020 개인정보보호 연차보고서>에서도 최근 개인정보 보호 주요 이슈로 '정보주체의 실질적 권리보장을 위한 동의제도 개선'을 포함하면서 "신기술 환경에서는 개인정보의 수집·이용·공유 등에 대한 사용자의 동의 요건이 매우 복잡하여 사전동의를 적용하는 것이 사실상 불가능" 해지고 있고 "정보주체가 해당 서비스를 이용해야 할 경우 동의가 필수이기 때문에 동의서 내용 등을 제대로 살펴보지 않고 형식적으로 동의하는 경우가 일반적이라는 의견이 많다"며 "소비자 또는 이용자가 쉽게 이해할 수 없는 기술적 기반과 비즈니스 모델을 추구하는 오늘날의 기술환경을 고려하여 정보주체의 동의 기반 보호 체제에 대해서도 예외적 Opt-out 인정 등 다양한 개선방안을 모색할 필요가 있다" 고 제안하고 있다[223].

정보주체의 동의는 정보주체가 개인정보에 대한 통제권을 행사하기 위한 중요한 수단임은 틀림없다. 인터넷 기업과 같은 개인정보처리자 입장에서는 정보주체의 권리보호를 위한 다양한 조치들을 하나의 규제로 인식하는 경향이 있다. 동의 제도에 대한 비판의 초점도 제각각이다. 따라서 현행 동의 제도가 문제가 있다면 무엇이 문제인지, 그러한 문제의 원인은 무엇인지, 제시되고 있는 해결책은 문제에 대한 해결과 연결이 된 것인지, 아니면 동의 제도의 문제를 빌미로 정보주체의 권리를 보호하기 위한 제도를 없애려는 것인지 신중하게 검토할 필요가 있다.

1. GDPR의 동의제도

GDPR에서 동의는 제6조에서 규정하고 있는 적법 처리의 근거 중의 하나이다. GDPR 하에서 적법한 개인정보 처리가 되기 위해서는 (a) 정보주체가 동의한 경우 (b) 계약 이행 혹은 계약 체결 전 정보주체의 요청에 따른 조치를 취하기 위해 필요한 경우 (c) 컨트롤러의 법적 의무준수 (d) 정보주체 또는 제3자의 핵심적 이익 보호 (e) 공익 혹은 컨트롤러의 공식 권한 행사를 위한 업무수행에 필요 (f) 컨트롤러 또는 제3자의 정당한 이익(정당한 이익이 정보주체의 이익 또는 기본적 권리와 자유보다 우선하는 경우) 중 하나의 요건을 충족해야 한다.

GDPR은 제7조에서 적법한 동의 조건을 상세하게 규정하고 있다. 즉, 컨트롤러는 정보

223) 개인정보보호위원회(2020), 2020 개인정보보호 연차보고서.

주체가 자신의 개인정보 처리에 동의하였음을 ‘입증’ 할 수 있어야 하고, 서면으로 이루어지는 경우 동의 요청은 “기타의 사안과 분명히 구별되는 방식으로, 이해하기 쉽고 입수가 용이한 형태로, 명확하고 평이한 문구를 사용한 방식”으로 제시되어야 한다. 정보주체는 언제든 자신의 동의를 철회할 수 있고, 동의의 철회는 동의의 제공만큼 용이해야 한다. 또한, “동의가 자유롭게 제공되는지 여부를 평가할 때, 무엇보다 서비스 제공 등의 계약의 이행이 해당 계약의 이행에 필요하지 않은 개인정보의 처리에 대한 동의를 조건으로 하는지 여부를 최대한 고려해야 한다”고 규정하고 있는데, 이는 계약을 빌미로 동의를 강제하지 말라는 것이다. 계약 이행과 동의는 서로 다른 법적 근거이며 이를 모호하게 혼합해서는 안된다[224].

동의의 형식을 갖춘다고 모두 진정한 동의가 되는 것은 아니다. GDPR 제4조 제11항은 동의를 “본인과 관련된 개인정보의 처리에 대해 합의한다는 개인정보주체의 희망을 진술 또는 명백한 적극적인 행위를 통해 자유롭고(freely given), 구체적으로 특정된(specific), 정보에 기반한(informed), 모호하지 않은(unambiguous) 의사표시”로 정의하고 있는데, 유효한 동의가 되기 위해서는 이러한 요건을 모두 충족해야 한다. 29조 작업반의 동의 가이드라인은 이러한 각각의 요소에 대해 상세하게 해설을 제공하고 있다[225].

한편, GDPR 제9조는 특정 범주의 개인정보, 즉 민감정보의 처리를 원칙적으로 금지하면서, 민감정보의 처리가 허용되는 몇 가지 예외를 규정하고 있는데, 정보주체가 명시적인(explicit) 동의를 제공한 경우가 그 중 하나이다. 즉, 민감정보의 처리에 대해 동의를 받을 때에는 일반적인 동의의 요건보다 강화된 요건을 적용하는데, 이때 ‘명시적인(explicit)’은 정보주체의 동의가 표현되는 방식을 의미한다. 가장 확실한 방법은 서명과 같이 문서로 동의 의사를 표현하는 것인데, GDPR이 이러한 형식만을 허용하는 것은 아니다. 예를 들어, 온라인 환경에서도 온라인 양식을 채우거나 이메일을 보내거나, 서명을 담은 문서를 스캔하여 업로드하거나 전자 서명을 이용하는 등 다양한 방식을 사용할 수 있으나, 명시적인 동의임을 입증할 책임은 컨트롤러에게 있다[226].

---

224) ARTICLE 29 DATA PROTECTION WORKING PARTY(2018b), Guidelines on consent under Regulation 2016/679, 17/EN WP259 rev.01. Adopted on 28 November 2017, As last Revised and Adopted on 10 April 2018, pp8-10.
225) Ibid.
226) Ibid, pp18-19.

2. 우리나라 개인정보 보호법상 동의제도

우리나라 개인정보 보호법도 GDPR과 유사하게 제15조에서 개인정보 수집의 근거를 두고 있다. 다만 GDPR의 경우에는 수집과 제공을 구분하지 않고 제6조에서 개인정보의 적법 처리 근거를 두고 있고, 이에 반해 우리나라 개인정보 보호법은 제15조에서 개인정보 수집·이용의 근거, 제17조에서 개인정보 제공의 근거를 두고 있다. 정보주체의 동의는 제15조 제1항에서 규정하고 있는 수집·이용의 근거 중 하나이며, 그 외에 법률에 특별한 규정이 있거나 법령상 의무 준수(제2호), 공공기관이 법령상 소관 업무수행을 위해 불가피한 경우(제3호), 계약의 체결 및 이행(제4호), 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 경우(제5호), 처리자의 정당한 이익, 단 명백하게 정보주체의 권리보다 우선하는 경우(제6호) 등을 근거로 수집 및 이용할 수 있는데, 이는 GDPR 제6조의 적법 처리 근거와 유사하다.

다만, 정보통신서비스 제공자의 경우에는 동의가 원칙이다(제39조의3 제1항). 서비스 제공 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우, 요금정산을 위해 필요한 경우, 다른 법률에 특별한 규정이 있는 경우에는 동의 없이 이용자의 개인정보를 수집·이용할 수 있도록 하고 있다(제39조의3 제2항). 이는 기존 정보통신망법 제22조를 개인정보 보호법으로 옮겨온 것인데, 이를 제15조 일반조항과 비교해 보면 제15조 제1항 제4호의 계약의 체결 및 이행, 제6호의 처리자의 정당한 이익에 근거한 개인정보 수집·이용이 정보통신서비스 제공자에게는 제한되는 것으로 볼 수 있다. 즉, 정보통신서비스 제공자의 경우에는 계약의 체결 및 이행을 개인정보 수집 근거로 할 수 없으며, 통상 정보주체의 동의에 기반하여 수집·이용할 수 있되 계약의 이행을 위해 필요하면서도 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우에만 동의를 받지 않고 수집할 수 있다는 것이다. 제39조의3이 정보통신서비스 제공자와 이용자 사이의 관계만을 규율한다는 점을 고려하면 제15조 제1항 제3호는 공공기관과 관련된 조항이므로 정보통신서비스 제공자와 관계없고, 제5호는 통상적인 정보통신서비스의 이용 관계에서는 크게 관련이 없는 조항이라고 보여진다.

한편, 제17조 제1항 개인정보 제공의 적법 근거도 정보주체의 동의를 비롯해서 수집·이

용의 적법 근거와 유사하지만, 계약의 체결 및 이행, 처리자의 정당한 이익은 개인정보 제공의 근거에서 제외되어 있다.

동의를 받는 방식과 관련하여 GDPR 제7조와 유사한 조항을 우리나라 개인정보 보호법은 제22조에 두고 있다. 개인정보처리자는 동의를 받을 때 '각각의 동의 사항을 구분'하여 '정보주체가 이를 명확하게 인지할 수 있도록 알리고' 각각 동의를 받아야 한다. 각각의 동의 사항을 구분해야 한다는 것은 GDPR에서 동의를 받을 때 처리 목적이 특정(specific)되어야 한다는 조건에 대응된다. GDPR 및 국내 개인정보 보호법 모두, 서로 다른 처리 목적에 대해 포괄적으로 동의를 받는 것을 허용하지 않고 특정한 처리 목적에 대해 각각 개별적으로 동의를 받도록 하고 있다. 또한 동의 요청은 이용자에게 명확하게 인지되어야 한다[227]. 또한 제22조 제2항은 동의를 서면으로 받을 때에는 중요한 내용을 보호위원회가 고시로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하도록 하고 있다. 개인정보처리자는 계약 체결 등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분해야 하며(제22조 제3항), 특히 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다(제22조 제4항). 또한 선택 사항에 대해 동의하지 않았다고 하여 정보주체에게 재화나 서비스의 제공을 거부해서는 안된다(제22조 제5항).

또한 민감정보 및 고유식별정보를 처리하고자 할 경우 다른 개인정보의 처리에 대한 동의와 '별도의 동의'를 받아야 한다(제23조 제1항 1호, 제24조 제1항 1호).

227) 홈플러스가 1mm 크기의 글씨로 개인정보 수집/이용목적 등이 기재된 경품 응모권을 통해 개인정보를 수집하고 이를 제3자에게 제공한 사건에서 대법원은 이와 같은 방식으로 동의를 받는 것은 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 하여야 한다는 개인정보 보호법상의 의무를 위반한 것으로 보았다. 서울중앙지방법원 2018. 8. 16. 선고 2017노1296판결, 대법원 2019. 7. 25. 선고, 2018도13694판결로 확정.

3. 현행 우리나라 동의제도의 문제점

현행 동의제도에 대한 가장 큰 비판은 동의 절차가 형식적이라는 점이다. 즉, 대다수의 정보주체는 약관이나 개인정보 처리방침 등 자신이 동의하는 내용에 대해서 제대로 읽어보지 않고 동의를 하는 경우가 많다는 것이다. 한 설문조사에 따르면 온라인에서 약관의 내용을 읽어보지 않고 서명만 하는 경우가 42%, 대충 훑어 읽어보고 서명하는 경우가 24%에 이르며, 꼼꼼히 읽어보고 서명하는 비율은 4%에 불과했다. 제대로 읽지 않는 이유는 약관의 내용이 너무 길거나 양이 많아서, 약관의 내용을 읽든 안읽든 상관 없이 동의해야 하기에 읽을 필요가 없다는 응답이 높게 나왔다[228].

이를 동의의 역설이라고 부르기도 한다. 즉, 개인정보처리자는 동의를 받기 전에 정보주체에게 충분한 정보를 제공하여야 하고, 정보주체의 동의는 명시적이고 개별적으로 이루어져야 하는데, 역설적으로 이는 동의를 더욱 형식적으로 만드는 원인이 된다는 것이다. 충분한 정보를 제공하고자 할수록 개인정보 처리방침이나 관련 약관은 복잡하고 길어지며, 개별 사항들에 대해 사전에 명시적이고 개별적인 동의를 받고자 할수록 동의를 위해 거쳐야 할 절차는 늘어나기 때문이라는 것이다. 최소 수집 원칙에도 불구하고 동의가 있으면 그 이상의 개인정보를 수집하는 것이 가능해지므로, 동의가 형식화되면 개인정보에 대한 통제권이 사실상 개인정보처리자에게 넘어갈 수 있다[229]. 다만 현재의 동의 원칙 자체가 필연적으로 동의의 역설을 불러오는 것인지는 검토해볼 필요가 있다. 왜냐하면 현재 동의가 형식화되고 있음을 인정한다고 하더라도, 동의의 원칙을 준수하면서 동의를 실질화하기 위한 다른 방법이 존재할 수 있기 때문이다.

현행 동의제도에 대한 또 다른 비판은 사물인터넷과 같은 기술환경에 적용하기 힘들다는 점이다. 사람이 개입하지 않고 정보가 수집, 이용되는 사물인터넷 체제하에서는 사전에 정보주체로부터 일일이 개인정보 수집과 이용에 대한 동의를 받는 것이 거의 불가능하며, 따라서 그러한 동의를 받도록 법적으로 강제하는 동의 제도는 사물인터넷과 관련된 기술의 발전에 장애가 될 수 있다는 것이다[230]. 이러한 경우에도 현행법에 따르면

228) 나종연(2013), 정보주체 동의권의 실질적 보장을 위한 연구, 서울대학교 산학협력단, 개인정보위원회 연구용역보고서, p12.
229) 권영준(2015), 개인정보 자기결정권과 동의 제도에 대한 고찰, 2015 NAVER Privacy White Paper, pp124-125.
230) 권영준(2015), 위의 글, p126

원칙적으로 동의를 받거나 아니면 다른 법적 근거가 있어야 하는데 개별적인 서비스나 신기술마다 개별적인 법적 근거를 신설하는 것도 바람직한 방향은 아니고 실현 가능하지도 않다[231].

한편, 국내 동의제도는 지나치게 엄격하고 복잡하다는 비판도 제기된다. 즉, 수집·이용·제공·위탁(정보통신망법의 경우) 각각의 경우에 동의를 받을 것을 요구하고 있을 뿐 아니라, 원칙적으로 수집 및 이용에 대한 동의와 제공 동의, 위탁 동의를 구분해서 개별적으로 동의를 받아야 하는데다 필수 동의사항에 대해서도 사전동의를 받을 것을 강제하고 있다는 것이다. 또한 복잡한데 개인정보 보호법과 정보통신망법은 물론, 신용정보법, 나아가 위치정보의 보호 및 이용 등에 관한 법률까지 정보보호에 관한 법률이 지나치게 다양하고 규정도 상이하여 수범자로 하여금 혼란스럽게 한다는 것이다[232]. 그런데, 이미 정보통신망법의 경우 개인정보 보호법으로 일원화되어 위탁 동의 문제는 해결되었고, 서로 다른 법률에 따른 혼란은 동의제도에 한정된 문제는 아니다. 다만, 개인정보의 수집, 이용과 제공의 적법 근거를 따로 규정할 필요가 있는지에 대해서는 검토해볼 필요가 있다. 또한 GDPR 역시 사전동의, 처리 목적에 따른 동의 등 유효한 동의에 대해 엄격한 요건을 두고 있다는 점에서 우리나라의 동의제도만 엄격한 것은 아니라는 점을 지적할 필요가 있다.

우리나라의 법에서는 개인정보 처리에 대한 동의 시 고지한 법정 고지사항이 변경되는 경우에도 다시 동의를 받도록 하고 있고, 법정 고지사항에 대해 엄격하게 규정하고 있는 현행법 및 이를 더 엄격하게 해석하는 실무의 태도와 맞물려 정보 활용 범위를 크게 제한한다는 점, 동의 규범 위반 시에 형사 제재를 가하고 있다는 점 역시 지적되고 있다[233]. 그러나 이에 대해 한편으로는 대부분 사업자들이 재동의를 받지 않고 개인정보 처리방침을 개정해오고 있다는 점, GDPR에서도 처리 목적 등 중요한 사항이 변경되면 당연히 다시 동의를 받아야 한다는 점에서 과연 우리나라 동의제도의 독특한 문제인지는 의문이다. 형사처벌 문제는 그보다 실효성 있는 제재 방안은 무엇인지에 검토와 함께 동의 문제를 떠나 별개로 검토할 필요가 있다.

---

231) 최경진(2017), 4차 산업혁명 시대의 개인정보보호법제 개선방안, 법제연구 제53호, pp191-192.

232) 고환경 외(2019), MyData 서비스의 개인동의 방식 개선 연구, 한국데이터산업진흥원 위탁연구보고서, p42.

233) 고환경 외(2019), 위의 글, p43.

4. 개선방안

그렇다면 형식화 되어 있는 현행 동의제도를 어떻게 개선해야 할까. 우선 정보에 기반한 동의(informed consent)를 실질화하는 방안을 모색할 필요가 있다. 현재의 동의제도가 작은 글씨와 법률 문서로 이루어진 개인정보 처리방침을 강제하고 있는 것은 아니다. GDPR은 이해하기 쉽고 명확하고 평이한 문구를 사용하도록 하고 있고 아이콘과 같은 이미지를 사용할 수도 있다. 우리나라 개인정보 보호법 역시 정보주체가 명확하게 인지할 수 있도록 알리도록 하고 있다. 중요한 내용은 단순하고 명확하게 전달하면서도 원하는 사람은 찾아볼 수 있도록 전체 정책에 접근하는 방법을 제공할 수도 있다. 중요한 것은 정보주체에게 실질적이고 효율적으로 정보를 제공하는 방법을 모색해야 한다는 것이다[234].

유형고지를 도입하자는 제안도 있다[235]. 유럽연합에서도 유형고지를 인정하고 있는 것으로 보인다. 다만, 완전히 유형고지로 전환할 경우 정보주체가 실제 업체명을 알고 싶을 경우 정보가 제한될 수 있고, 이를 악용하여 실제 중요한 고지 내용이 드러나지 않을 수도 있다. 이를 앞서 언급한 내용과 결합하자면, 단순하게 전달하는 버전에는 유형고지를 사용하고 개인정보 처리방침의 상세 버전에서는 현재와 같이 실제 업체명을 표기하는 방안이 대안이 될 수 있다.

이와 병행하여 소비자단체, 개인정보 보호위원회, 소비자보호원 등 전문기관들이 주요 개인정보처리자들의 약관이나 개인정보 처리방침이 문제가 있는지 사전에 검토할 수도 있다. 문제가 있는 불공정 약관에 대해서는 시정하도록 요구할 수도 있고, 적절한 약관이나 개인정보 처리방침을 채택하고 있는 처리자를 인증할 수도 있다. 현재 개인정보 보호법은 인증제도를 두고 있는데, 인증 범위를 확대하여 개인정보 처리방침에 대한 인증제를 시행할 수도 있을 것이다[236]. 이를 통해 정보주체가 꼼꼼하게 읽지 않더라도 부당한 약관을 걸러낼 수 있을 것이다.

현행 동의제도 개선과 관련하여, 포괄동의로 전환하자는 의견도 제기된다[237]. 나아가

---

234) 권영준(2015), 앞의 글, pp132-133.
235) 고환경 외(2019), 앞의 글, p46.
236) 권영준(2015), 앞의 글, pp134-136.
237) 인벤, 2019.11.14., “인터넷기업협회 "게임 관련 관계자들의 상생 플랫폼 만들겠다", <http://m.inven.co.kr/webzine/wznews.php?idx=229805>.

사전 규제로서의 동의 규제나 각종 형식 규제는 과감히 축소하거나 처벌 없는 규제로 전환하여 보다 자유롭게 합법적으로 개인정보를 활용할 수 있는 길을 열어주고, 사후적으로 개인정보의 오남용에 대한 강력한 제재를 가하는 체계로 전환하자는 제안도 있다[238]. 그러나 포괄동의로 전환하거나 사전 규제를 없애는 것이 어떻게 정보주체의 보호로 이어지는지 납득하기 어렵다. 사후적으로 개인정보 오남용에 대해 강력히 제재하자는 것은 사전 동의제도와 양립할 수 없는 것이 아니다. 당연히 동의제도가 있더라도 개인정보처리자의 책임성 강화와 강력한 처벌을 병행할 수 있고 실제로 GDPR이 그렇게 하고 있다.

둘째, 동의 외에 개인정보 수집을 위한 다른 적법 근거를 활용할 필요가 있다. 앞서 언급한 설문조사에서도 나타난 것처럼 시민들이 동의 절차에 대해 불필요한 것으로 느끼는 이유 중의 하나는 어차피 개인정보를 제공할 수밖에 없는 상황에서 동의에 클릭하게 하는 절차가 추가되었기 때문이다. 예를 들어, 어떤 앱을 쓰기 위해서 필수적인 정보의 경우에는 앱을 쓰기로 했다면 당연히 제공할 수밖에 없다. 개인정보를 제공하기 원하지 않는다면 앱을 사용하지 않으면 된다. 혹은 어떤 물품을 택배로 배달받으려면 자신의 주소를 제공할 수밖에 없다. 주소를 제공하지 않고 배달을 요청할 수는 없는 것이다. 당연한 절차에서 동의를 요구하는 것은 정보주체에게 불필요한 것으로 느껴질 수밖에 없다. 물론 동의 여부와 무관하게 개인정보의 처리 목적, 개인정보처리자의 정보 등 동의를 받을 때 정보주체에게 제공해야 할 정보는 이 경우, 즉 계약의 이행을 위해 개인정보를 제공하는 경우에도 제공해야 하며, 정보주체의 다른 권리도 당연히 보장되어야 한다.

때로는 법령에 근거한 의무 이행을 위해 수집된 개인정보를 정보주체의 동의 없이 처리할 수도 있다. 예를 들어, 수사기관이 법원의 영장에 근거해 요청할 경우가 이에 해당한다. 때로는 개인정보처리자의 정당한 이익이 개인정보 처리의 근거가 될 수 있다. IP 주소 역시 개인정보이기는 하지만 로그기록에 남는 접속자의 IP 주소를 동의를 받고 수집하기는 힘들다. 쇼핑몰에서 판매 현황을 분석하는 경우에도 소비자의 개인정보가 처리되기는 하지만, 이는 상품 배송을 위한 처리와는 다른 목적이므로 별도의 법적 근거를 가질 필요가 있다.

많은 사람들이 우리나라 개인정보 보호법은 수집 및 처리의 법적 근거로 지나치게 동

238) 최경진(2017), 앞의 글, p202.

의에 의존한다고 생각하는 이유 중 하나는 정보통신망법에서 개인정보 수집 및 제공의 근거를 개인정보 보호법보다 제한적으로 규정했기 때문이다. 즉, 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우, 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우, 이 법 또는 다른 법률에 특별한 규정이 있는 경우 외에는 정보주체의 동의에 근거해서만 개인정보를 수집·이용할 수 있고, 다른 법률에 특별한 규정이 없는 경우 동의에 근거해서만 개인정보를 제3자에게 제공할 수 있도록 했기 때문이다. 개인정보 보호법 내의 '정보통신서비스 제공자 등의 개인정보 처리 등 특례' 규정으로 편입된 현재에도 수집·이용과 관련해서는 기존의 규정을 유지하고 있다. 이와 같은 정보통신망법의 규정은 동의제도 문제와 무관하게 개인정보 보호법의 관련 규정과 통합될 필요가 있다.

이러한 통합을 전제로 보면, 개인정보 보호법 제15조는 GDPR과 유사하게 동의 외에도, 개인정보의 수집 및 처리를 위한 적법 근거를 제공하고 있다. 법률 규정 혹은 법령상 의무(제15조 제1항 제2호), 공공기관의 소관업무 수행을 위해 불가피한 경우(제3호), 계약의 체결 및 이행(제4호), 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 경우(제5호), 개인정보처리자의 정당한 이익(제6호) 등이다. '정당한 이익'의 경우에 대해서는 GDPR과 달리 한국은 '명백하게' 정보주체의 권리에 우선해야 하기 때문에 이 조항의 적용이 제한적이라는 비판도 있지만[239], 결국 '정당한 이익'인지 여부를 1차적으로 판단하는 것은 정보주체가 아니라 개인정보처리자이기 때문에 개인정보처리자의 편향적인 판단 가능성을 고려할 필요가 있다는 점에서, 정당한 이익 조항이 개인정보의 동의 없는 수집을 정당화하는 수단으로 남용되지 않도록 하기 위해서는 '명백하게'라는 표현을 유지하는 것이 바람직할 것으로 본다.

이처럼 동의 외에 다양한 적법 근거를 인정하기 위해서는 몇 가지 전제가 필요하다. 우선 서비스 제공을 위해 필수적인 개인정보의 경우 계약의 체결 및 이행 조항을 수집 근거로 활용하더라도 필수적이지 않은 정보를 수집하고자 한다면 동의 등 다른 법적 근거가 필요하다. 또한 민감정보 및 고유식별정보에 대한 별도의 동의 요건은 유지되어야 한다. 정보주체에 대한 고지 의무도 강화될 필요가 있다. 정보주체의 입장에서 현재 동

239) 고환경 외(2019), 앞의 글, p67-73.

의에 의존할 수밖에 없는 이유는 GDPR과 달리 우리나라 개인정보 보호법은 동의를 받을 경우에만 처리의 목적이나 개인정보처리자의 신원 등 관련 정보를 제공하도록 하고 있기 때문이다. 이렇게 해서는 동의 외에 다른 법적 근거를 통해 개인정보를 수집할 경우 정보주체가 자신의 개인정보가 수집되었다는 사실, 그리고 이와 관련된 자신의 권리도 명확하게 인지하기가 힘들게 된다. 따라서 동의가 아닌 다른 법적 근거에 따라 개인정보가 수집 및 처리되더라도 개인정보 처리와 관련된 정보들을 정보주체에게 제공하도록 개인정보 보호법이 개정되어야 한다. 더불어 동의에 기반할 경우 정보주체가 언제든지 동의를 철회할 수 있는 것과 같이, 정보주체의 동의에 기반하지 않을 경우에는 정보주체가 언제든 개인정보의 처리를 반대하거나 처리정지를 요구할 수 있는 권리를 보장해야 한다. 예를 들어 동의 없이 과학적 연구목적으로 제공하거나 정당한 이익에 근거해서 처리하는 경우 등이 이에 해당한다. 개인정보가 동의에 근거해서 처리되지 않을 때에도 정보주체는 자신의 개인정보가 수집, 처리되고 있다는 것과 다른 법령에 처리를 강제하는 근거가 없는 한 언제든지 처리의 정지를 요구할 권리가 있다는 것을 명확하게 인지할 수 있어야 한다.

개인정보 처리방침에도 처리하는 개인정보에 따라, 혹은 처리 목적에 따라 법적 근거가 무엇인지 개별적으로 밝혀줄 필요가 있다. 예를 들어, 영국 런던에 주소지를 두고 있는 언론사인 가디언의 경우 개인정보 보호정책[240]에서 동의, 계약 이행, 법의 준수, 정당한 이익 등 서로 다른 개인정보 처리에 대한 법적 근거를 제시하고 있다. 마케팅 이메일 발송은 동의에 근거하고, 구독자의 연락처와지불 정보의 처리는 계약 이행에 근거하며, 사이트나 앱에서 읽혀진 콘텐츠의 분석은 정당한 이익에 근거를 둔 것이다. 프랑스에 기반한 음악 스트리밍 서비스업체인 디저(deezer)의 경우에도 개인정보 보호정책[241]에서 처리 목적에 따라 서로 다른 법적 근거를 제시하고 있다.

셋째, 사물인터넷이나 자율주행자동차와 같이 만일 일일이 동의를 받는 것이 불가능한 경우는 어떻게 해야 할까? 아마도 이에 대처할 수 있는 여러 방식이 있을 수 있을 것이다. 예를 들어 고정형 CCTV의 경우 일반적인 개인정보 처리와 구별되는 별도의 규정을 이미 개인정보 보호법에 두고 있다. 이처럼 별도의 규정이 필요할지, 아니면 기존의 적

240) Guardian, 2020.11.23., “Privacy policy”, <https://www.theguardian.com/help/privacy-policy>.
241) deezer, 2020.5., “Privacy policy”, <https://www.deezer.com/legal/personal-datas>.

법 처리 근거를 활용 가능할지는 실제 사례에 따라 달라질 것이다. 물론 새로운 기술이나 상품이 나타날 때마다 법적 근거를 새로 만드는 것이 쉽지 않을 수 있다. 현재로서는 어떠한 결론을 내리기 이전에, 새로운 기술이나 서비스가 기존의 동의제도와 어떻게 충돌하는지 추가적인 연구가 필요해 보인다. 구체적인 근거 없이 동의제도를 회피하기 위한 목적으로 사물인터넷 등의 새로운 기술환경이 근거로 활용되어서는 안 된다. 사물인터넷 환경이 도래할 것이므로 옵트아웃 방식으로 전환하자는 주장은 지나친 논리적 비약이다.

넷째, 법 위반 행위에 대한 강력한 처벌 등 동의 이외에 개인정보 보호를 위한 사회적 통제의 강화도 제안되고 있다. 또한 개인정보의 정정이나 파기 또는 법적 책임 추궁과 같은 이용 단계에서의 사후적 통제, 프라이버시 증진 기술(privacy enhancing technologies, PETs)을 활용한 기술적 통제, 민간영역에서의 자율통제 등을 통해 더욱 실질적인 개인정보 보호가 이루어질 수 있다는 의견도 있다[242]. 당연히 정보주체의 권리를 보호하기 위한 방안은 동의제도에 한정되어서는 안 된다. 개인정보 처리의 전 과정에서 개인정보를 안전하게 보호하고 개인정보처리자의 책임성을 강화할 수 있는 법제가 구축될 필요가 있으며, 이와 관련된 기술적인 보호 조치들도 수반되어야 할 것이다. 다만, 이러한 보호 조치들은 동의제도와 양립할 수 없는 것이 아니며, 동의제도를 약화시키기 위한 명분으로 이해되어서도 안 된다.

242) 권영준(2015), 앞의 글, p144.

제5장 개인정보처리자의 책임성 강화

제1절 컨트롤러, 프로세서, 공동 컨트롤러의 개념과 책임 강화

1. 개요

오늘날 디지털 플랫폼 기업은 수집한 개인정보를 수많은 애플리케이션 등을 통해서 다수의 제3자들과 긴밀하게 공유하거나, 제공하고 있다. 그 과정에서 개인정보를 전문적으로 처리하는 여러 기업들이 다양한 역할을 하기도 한다. 그뿐만 아니라 클라우드 서비스나 IoT 서비스의 데이터 처리와 같이 제3자가 전문적으로 개인정보 처리를 담당하는 분야도 확산되고 있다. 이와 같이 개인정보 처리와 관련한 주체들의 관계가 복잡해지면서 특정한 개인정보 처리를 누구의 개인정보 처리로 볼 것인지가 중요한 문제가 되고 있다.

이와 같이 개인정보 처리와 관련하여 관여되어 있는 복잡한 주체들에 대하여, 개인정보 처리와 관련한 여러 가지 의무를 부담하여야 하는 주체인 개인정보처리자를 누구로 볼 것인지는 매우 중요한 문제이다.[243] 그에 따라서 (i) 누구를 기준으로 처리에 대한 동의를 받거나, 법적 근거를 갖추어야 할 것인지, (ii) 누가 여러 가지 안전조치 등의 책임을 질 것인지, (iii) 개인정보 주체의 권리 행사의 상대방은 누구로 할 것인지 등의 문제가 결정되는 것이기 때문이다. 이것은 개인정보주체에게나 개인정보를 처리하는 자에게나 개인정보 보호 법제를 통해서 개인정보의 안전한 처리와 정보주체의 권리를 보장하려는 정책을 결정하는 자에게나 가장 먼저 결정해야 하는 매우 기본적이고 중요한 문제이

243) 그 중 특히 개인정보 컨트롤러는 여러 책임과 의무를 준수해야 하고, 손해배상 책임과 과징금이나 형사처벌 등의 부과 대상으로 핵심적인 역할을 하는 주체이다. 그래서 GDPR은 개인정보 컨트롤러를 개인정보 처리의 목적과 수단을 결정하는 자로 정의하면서 개인정보 처리의 목적과 방법을 결정하고, 지시하는 자의 책임을 강조하고, 개인정보 컨트롤러와 프로세서를 구분하는 기준을 발전시켜 가고 있다. 아울러 현실의 다양한 운용 방식을 고려하여, 공동으로 개인정보 처리의 목적과 수단을 결정하는 자를 공동 컨트롤러로 보고, 그에 대하여는 연대책임 등 책임성을 강화하고 있다. 아울러 컨트롤러와 프로세서의 관계에 있어서도 안전한 처리를 충분히 보장할 수 있는 자를 프로세서로 이용할 의무를 부과하고, 계약의 서면주의 등 책임성을 강화하기 위한 다수의 규정을 도입하였다. 이는 현실에 조응하는 책임과 의무 체계를 갖추기 위한 노력이다.

다.

실제로 개인정보 처리에 관여하는 주체들 사이에서는 누구를 개인정보처리자로 볼 것인지, 누가 처리에 대한 동의나 법적 근거를 갖추어야 하는지, 누구에게 권리 행사를 할 것인지의 문제는 첨예한 쟁점이 되고 있다.[244] 따라서 개인정보 처리에 관여되는 주체들 사이의 관계, 누구를 기준으로 개인정보 처리에 대한 동의를 받거나, 법적 근거를 갖출 것인지, 개인정보 처리와 관련한 의무의 주체, 처리자들 사이의 책임 관계를 명확하게 하기 위한 조치의 내용들에 대해 명확한 규정이 마련될 필요가 있다.

이와 관련하여 유럽연합은 개인정보가 처리되는 복잡성을 고려하여 GDPR을 통하여 기존의 디렉티브(95/46/EC)를 보다 구체화하고, 구별기준을 명확하게 마련해 나가고 있다. 아울러 개인정보주체의 권리 보호와 안전한 개인정보의 처리를 위하여 개인정보의 처리를 제3자에게 맡기는 것과 관련해서는 엄격한 요건과 규율을 마련하고 있고, 처리 활동 기록 의무나, 서면 계약서 작성 의무, 서면 지시 의무 등을 도입하여 투명성을 강화하고 있다. 즉, 개인정보 처리와 관련되어있는 자들을 컨트롤러, 공동 컨트롤러, 프로세서, 수령인, 제3자라는 개념 체계로 구분하고 그 구별기준을 현실에 맞춰서 지속적으로 세분화, 구체화하고 있으며, 새롭게 여러 개의 조문을 신설하여 컨트롤러와 프로세서의 관계를 꼼꼼하게 규율하고 있다.

반면 우리나라 개인정보 보호법은 관련 규정이 매우 간략한데다가 구별 기준도 마련되어 있지 않는 등 개인정보 처리의 복잡한 현실을 반영할 수 있는 체계로 발전시켜 나가는데 있어서 미흡한 점이 많다. 개인정보처리자와 수탁처리자, 개인정보취급자의 개념에 있어서도 개인정보처리자를 개인정보파일을 운용하는 자로 규정하여 개인정보 처리에 초점을 맞추고 있고, 그 기준의 세부화를 위한 노력도 보이지 않아 왔다. 그리고 개인정보 수탁처리에 있어서는 수탁처리자의 책임을 개인정보처리자 규정을 준용하도록 강화하면서도, 개인정보처리자와 수탁처리자의 관계에 있어서 위수탁계약의 체결과 이행에 관한 규율이 형식적이고, 개인정보 처리를 위탁하는 자의 책임에 대한 규정이 상대적으로 미흡한 실정이다. 이로 인하여 실질적으로 개인정보 처리의 목적과 방법을 결정하는 지

244) 예를 들어 페이스북은 최근 Cambridge Analytica 개인정보 불법 활용과 관련하여 이루어진 후속 조사에서, 자신들의 플랫폼에서 개인정보를 수집, 보유, 통합, 검색 등의 처리를 하고 있고, 제3자의 제휴 앱들이 해당 플랫폼에서 페이스북 이용자들의 개인정보를 열람, 조회 등을 할 수 있도록 허용하고 있는데, 이와 관련하여 페이스북은 해당 제3자들이 독자적인 개인정보 컨트롤러가 아니라 페이스북의 서비스를 이행하는 자로 보아야 한다는 주장을 하였다.

시자임에도 개인정보파일을 운용하는 자가 아니라고 판단되어 책임주체에서 배제될 가능성도 있고, 실질적으로는 개인정보 처리의 이익을 향수하면서 처리의 목적과 방법을 결정하는 자는 책임과 의무를 부담하지 않고, 그로부터 사실상의 실행 업무만을 수행하는 자가 책임과 의무를 모두 부담하고, 그 결과 실질적으로 정보주체에게 책임이 담보되지 않게 될 가능성도 크다.

따라서 이와 관련하여 우리나라의 개인정보 보호 법제에서도 GDPR의 해당 규정의 취지를 반영하여 개인정보 처리와 관련하여 책임과 의무를 정립하는 가장 기초가 되는 시발점인 개인정보처리자, 수탁처리자, 개인정보취급자의 개념을 재정비하고, 위수탁 등 제3자에게 처리를 맡기는 경우에 대한 투명성 강화와 책임성 강화를 위한 법제 개선을 하는 것이 필요하다.

2. 개인정보 처리와 관련한 주체들에 관한 규정

오늘날 개인정보 처리와 관련한 주체들의 관계가 복잡해지면서 특정한 개인정보 처리를 누구의 개인정보 처리로 보고, 누구를 기준으로 처리에 대한 동의를 받거나, 법적 근거를 갖추어야 할 것인지, 여러 가지 안전조치 등의 책임이나 개인정보 주체의 권리 행사의 상대방은 누구인지, 처리에 관여하는 주체들 사이에서는 어떻게 개인정보 처리에 대한 역할과 의무를 규정할 것인지 등 여러 문제가 제기되고 있다.

이와 관련하여 GDPR은 개인정보 처리와 관련한 주체들을 컨트롤러, 공동 컨트롤러, 프로세서의 개념으로 구분하고 있는데, 컨트롤러의 범위를 확대하고, 그 책임을 강화하고 있다. 아울러 프로세서를 활용하는 경우에 대해서도 컨트롤러에게 매우 엄격한 요건과 절차를 규정하여 컨트롤러의 책임성을 강화하고 있다.

가. GDPR의 규정

1) 컨트롤러와 프로세서, 공동 프로세서

GDPR은 1995년 디렉티브(Directive 95/46 EC)에서부터 유지해 온 개인정보 처리와 관련한 주체들로 컨트롤러, 프로세서, 수령자, 제3자의 구조를 유지하고 있다(제4조 (7)~

(10))[245]. 공동 컨트롤러는 1995년 디렉티브에는 명시적으로 규정하고 있지는 않고, 컨트롤러를 단독으로 또는 공동으로 할 수 있다고만 규정했었는데, GDPR에서 별도의 개념으로 도입하였다[246].

컨트롤러와 프로세서에게는 각각의 책임과 의무가 부과되는데, 컨트롤러, 프로세서의 명확한 의미와 그 구별의 기준은 GDPR의 적용에 있어서 가장 중요한 것으로 보고 있다. 이를 구별하는 기준을 좀 더 예측가능하고 명확하게 하기 위해서 각국의 개인정보 감독기관의 협의체인 제29조 작업반(Article 29 Working Party)은 2010년에 컨트롤러, 프로세서의 개념에 대한 가이드라인을 의견서를 통해서 발표하였고(의견서 1/2010, WP169[247]) GDPR의 도입 이후에는 EDPB에 의하여 새롭게 가이드라인을 발표하였다(가이드라인 07/2020[248]).

그 중 핵심적인 역할을 하는 자는 '컨트롤러'이다. GDPR은 '단독으로 또는 타인과 공동으로 개인정보 처리의 목적과 수단을 결정하는 자연인이나 법인, 공공기관, 기구 또는 기타 단체'를 컨트롤러로 규정하고 있는데(제4조 (7))[249], 정보 컨트롤러는 GDPR에서 여러 가지 책임과 의무, 손해배상 책임의 주체이고, 처벌의 대상이 되고 있다.

한편, 프로세서는 컨트롤러를 대신해 개인정보를 처리하는 자연인이나 법인, 공공기관, 기구 또는 기타 단체를 의미한다(제4조 (8))고 규정하고 있고, '수령자'는 제3자든 아니든 관계없이, 개인정보를 제공받는 자연인이나 법인, 공공기관, 기구 또는 기타 단체를 의미한다(제4조 (9))고 규정하고 있다[250]. 그리고 '제3자'는 정보주체, 컨트롤러, 프로세서, 그리고 컨트롤러나 프로세서의 직접적 권한에 따라 개인정보를 처리하도록 허가된 사람 외의 자연인이나 법인, 공공기관, 기구 또는 기타 단체를 의미한다(제4조 (10))고 규

245) 디렉티브 95/46 EC(1995)에서는 제2조 (d), (e), (f), (g) 참조.
246) 디렉티브 95/46 EC(1995)에서는 제2조 (d) 참조.
247) ARTICLE 29 DATA PROTECTION WORKING PARTY(2010a), Opinion 1/2010 on the concepts of controller and processor adopted on 16 February 2010, WP 169.
248) EDPB(2020) Guidelines 07/2020 on the concepts of controller and processor in the GDPR(Version 1.0), Adopted on 02 September 2020.
249) GDPR은 '그러한 처리의 목적과 수단이 유럽연합이나 회원국 법률에 의해 결정되는 경우, 유럽연합이나 회원국 법률은 정보 컨트롤러가 누구인지를 규정하거나 정보 컨트롤러 지명에 대한 구체적 기준을 규정할 수 있다'고 규정하고 있다(제4조 (7) 2문).
250) GDPR은 '하지만 유럽연합이나 회원국 법률에 따른 특정 조회라는 틀 내에서 개인정보를 수령할 수 있는 공공기관은 수령자로 간주되지 않는다. 그러한 공공기관에 의한 개인정보 처리는 해당 정보 처리의 목적에 따라 적용 가능한 정보 보호 규칙을 준수해야 한다.는 규정을 두고 있다(제4조 (9) 2문, 3문).

정한다.

2) 컨트롤러와 프로세서의 구별기준과 구체적인 사례

컨트롤러는 '개인정보 처리의 목적과 수단을 결정하는 자'이다. 어떤 경우를 '개인정보 처리의 목적과 수단을 결정한다'고 볼 수 있는지에 대해서는 해당 규정이 명시되었던 1995년의 디렉티브에서부터 제29조 작업반의 의견[251]이 있었고, 유럽연합의 기구와 조직들의 개인정보 처리에 대한 감독기관인 EDPS에서도 가이드라인[252]을 낸 것을 비롯해서 다수의 의견서, 가이드라인과 판례 등이 축적되어 있다. GDPR 시행 후에도 각국의 감독기관을 구성원으로 하여 운영하는 조직인 EDPB는 2020년 9월에 새로운 가이드라인을 발표하였다. 이 가이드라인과 의견서에서는 오늘날의 복잡한 개인정보 처리의 유형에 따라서 컨트롤러와 프로세서를 구분할 수 있는 기준을 많은 예시와 함께 들고 있다.

GDPR의 규정에서도 언급하고 있는 것처럼 컨트롤러는 개인정보 처리의 목적과 방법을 결정하는 자(determines the purposes and means of the processing of personal data)[253]이고, 프로세서는 결정된 바에 따라서 지시를 받아서 처리를 하는 자(processes personal data on behalf of the controller)[254]를 말한다. 이때 컨트롤러는 처리의 목적과 방법 모두를 결정해야 한다고 하는데, 그 의미는 '왜 처리를 하는가'(목적)와 '어떻게 처리를 하는가'(방법)를 결정하는데 영향력을 미치는 것을 말한다고 해석한다[255]. 이때 주요한 것을 결정하면 족하고, 사소한 것에 대해서는 결정권이 위임될 수 있다고 본다[256]. 따라서 프로세서도 개인정보 처리의 목적과 방법을 사소한 부분에 대해서는 결정권을 가지고 처리할 수 있다고 본다.

한편, 컨트롤러는 개인정보 처리의 목적과 방법을 결정하기는 하지만, 해당 개인정보에 접근하지 않는 경우도 있을 수 있다고 한다. 이런 경우에도 개인정보의 처리 목적과 방법을 결정한 자는 컨트롤러로 본다. 예를 들어 다른 기업이 수집한 정보를 통계로 처리하거나, 익명으로 처리한 것을 받더라도 처리의 목적과 방법을 결정하는 자가 컨트롤

251) ARTICLE 29 DATA PROTECTION WORKING PARTY(2010a), op. cit.
252) EDPS(2019), EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, Adopted on 07 November 2019.
253) 제4조 (7).
254) 제4조 (8).
255) EDPB(2020), op. cit., p13.
256) Ibid., pp13-14.

러라는 것이다[257]. 공동으로 결정하는 공동 컨트롤러의 경우에도 개인정보에 접근하지 않더라도 컨트롤러가 될 수 있다고 한다.

3) 공동 컨트롤러에 대한 규정

GDPR은 개인정보 처리가 복잡하게 이루어지는 현실을 반영하여 공동 컨트롤러에 대한 규정을 두고 있다. '복수의 컨트롤러가 공동으로 처리의 목적과 수단을 결정하는 경우, 그들은 공동 컨트롤러다'라고 규정하여 이들을 '컨트롤러'로서의 책임과 의무를 준수해야 함을 명시하고 있다(제26조 1항). 각 컨트롤러는 의무와 책임의 준수를 위하여 역할을 분담할 수 있지만 그 역할 분담은 약정을 통해서 투명하게 이루어져야 하고, 정보주체가 이용할 수 있도록 알려야 한다(제26조 2항). 그러나 정보주체는 공동 컨트롤러들 사이의 약정과 관계없이 각각에 대해서 GDPR에 의한 권리를 행사할 수 있다(제26조 3항).

나. 컨트롤러와 프로세서의 관계와 책임

GDPR은 컨트롤러가 프로세서에게 정보 처리를 맡길 경우, 그 요건과 방법 등을 상세하게 규정하고 있는데, 이는 컨트롤러의 프로세서에 대한 책임성과 정보주체에 대한 책임성을 강화하기 위한 것이다.

첫째, 컨트롤러는 '충분한 보증'을 제공하는 자를 프로세서로 이용할 의무를 진다. 즉, 컨트롤러는 자신을 대신한 처리 수행의 경우, 해당 처리가 GDPR 규정의 요구사항을 충족하게 되는 방식으로 적절한 기술적, 조직적 조치를 이행하며 정보 주체의 권리 보호를 보장한다는 충분한 보증을 제공하는 프로세서만을 이용해야 한다[258].

둘째, 프로세서 추가나 교체 시 서면 허가를 받을 의무를 부담한다. 프로세서는 컨트롤러의 사전 특정 또는 일반 서면 허가 없이 다른 프로세서를 참여시켜서는 안 된다. 이때 일반 서면 허가의 경우, 프로세서는 다른 프로세서 추가 또는 교체에 관한 변경 계획을 컨트롤러에게 고지해 정보 컨트롤러가 그러한 변경에 반대할 기회를 주어야 한다[259].

---

257) Case C-210/6, Wirtschaftsakademie Schleswig-Holstein, Ibid., p16.
258) 제28조 제1항
259) 제28조 제2항

셋째, 컨트롤러가 프로세서에게 처리를 맡기는 것과 관련한 엄격한 규율을 규정하고 있다. GDPR은 컨트롤러가 프로세서에게 처리를 맡기는 경우에는 법률 또는 계약에 의하여 명확하게 세부적인 사항까지 규정하여야 한다는 규율을 두고 있다. 즉, 해당 계약에는 처리의 대상, 기간, 처리의 성격과 목적, 개인정보의 유형과 정보 주체의 범주, 컨트롤러의 의무과 권리가 규정되어 있어야 하고, 컨트롤러의 서면 지시에 의해서만 개인정보를 처리해야 한다거나, 법률이 요구하는 모든 안전조치 의무를 준수해야 한다거나, 의무 준수를 입증하는 데 필요한 모든 정보를 컨트롤러에게 이용할 수 있게 하여야 한다는 등의 내용을 포함하여 다음과 같은 프로세서의 의무를 규정해야 한다[260].

(a) 컨트롤러의 서면 지시에 따라서만 개인정보를 처리한다. 여기에는 제3국 또는 국제기구로의 개인정보 이전과 관련한 경우도 포함한다. 단, 프로세서가 준수해야 하는 유럽연합이나 회원국 법률이 요구하는 경우는 예외이며, 그러한 경우, 프로세서는 처리 전에 컨트롤러에게 그러한 법적 요구사항을 고지해야 한다. 단, 해당 법률이 공익과 관련한 중요한 근거로 그러한 고지를 금지하는 경우는 예외이다.
(b) 개인정보를 처리하도록 허가된 사람이 기밀유지를 약속했거나 적절한 법적 기밀유지 의무를 지고 있는지 확인한다.
(c) 제32조에 따라 요구되는 모든 조치(안전조치)를 취한다.
(d) 다른 프로세서를 참여시키는 것에 관한 제2항(서면허가와 변경에 반대할 기회 제공) 및 제4항(동등한 의무 부과)에 언급된 조건을 존중한다.
(e) 처리의 성격을 고려하여, 제3장에 규정된 정보 주체의 권리 행사 요청에 대응해야 하는 컨트롤러의 의무를 충족할 수 있도록, 가능한 한 적절한 기술적, 조직적 조치를 통해 컨트롤러를 지원한다.
(f) 처리의 성격과 프로세서가 이용 가능한 정보를 고려하여, 제32조~제36조에 따른 의무준수를 보장하려는 컨트롤러를 지원한다.
(g) 컨트롤러의 선택에 따라, 처리에 관한 서비스 제공이 종료된 뒤 모든 개인정보를 삭제하거나 컨트롤러에게 반환하고, 기존 사본을 삭제한다. 단, 유럽연합이나 회원국 법률이 개인정보 보관을 요구하는 경우는 예외이다.
(h) 본 조에 규정된 의무준수를 입증하는 데 필요한 모든 정보를 컨트롤러가 이용할 수 있게 하고, 컨트롤러 또는 컨트롤러가 권한을 부여한 다른 감사관이 수행하는 감사(조사 포함)를 허용하고 이에 협조한다. 첫 번째 문단의 제(h)호와 관련하여, 프로세서는 지시가 본 규정 또는 다른 유럽연합이나 회원국 정보보호 규정에 위배된다고 생각될 경우 컨트롤러에게 바로 고지해야 한다[261].

260) 제28조 제3항
261) 제28조 제3항 (a) ~ (h)

넷째, 프로세서가 정보 컨트롤러를 대신한 특정 처리 활동 수행에 다른 프로세서를 참여시키는 경우, 컨트롤러와 프로세서 간 계약 또는 기타 법적 조치에서 규정된 것과 동일한 정보보호 의무가 계약 또는 기타 법적 조치를 통해 해당 다른 프로세서에게도 부과되어야 한다. 이는 특히, 처리가 본 규정의 요구사항을 충족하게 되는 방식으로 적절한 기술적, 조직적 조치를 이행한다는 충분한 보증을 제공해야 한다. 해당 다른 프로세서가 정보보호 의무를 충족하지 못할 경우, 원래의 프로세서는 해당 다른 프로세서의 의무 이행에 대해 컨트롤러에게 전적으로 책임을 져야 한다[262].

다섯째, 위와 관련한 계약 또는 기타 법적 조치는 서면(전자적 형태포함)으로 이루어져야 한다[263].

여섯째, 프로세서가 처리의 목적과 수단을 결정하여 본 규정을 위반한 경우, 해당 처리와 관련하여 프로세서를 컨트롤러로 간주해야 한다[264].

3. 우리나라 개인정보 보호법의 규정

가. 개요

우리나라 개인정보 보호 법제에서는 개인정보처리자, 수탁자, 개인정보취급자로 나누고 있으며, 공동으로 개인정보 처리를 결정하는 자에 대한 규정은 두고 있지 않다.

- 개인정보처리자 : 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등(개인정보 보호법 제2조 제5호)
- 수탁자 : 개인정보처리자로부터 개인정보의 처리 업무를 위탁받은 자(개인정보 보호법 제26조)
- 개인정보취급자 : 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자(개인정보 보호법 제28조 제1항)

즉, 개인정보 보호법은 개인정보파일을 운용하는 자를 개인정보처리자로 두고(제2조

262) 제28조 제4항
263) 제28조 제9항
264) 제28조 제10항

제5호), 개인정보처리자로부터 위탁을 받아서 처리 업무를 수행하는 자를 수탁자로 본다는 규정만을 두고 있으며, 위탁자와 수탁자의 관계에 대하여 단 한 개의 조문으로 간략하게 규율하고 있다[265].

개인정보처리자가 수탁자에게 개인정보 처리 업무를 위탁하는 경우에는 처리자는 처리자로서의 책임을 부담하고, 수탁자도 제15조 ~ 제25조, 제27조 ~ 제31조, 제33조 ~ 제38조 및 제59조가 준용된다(제26조 제7항). 한편, 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 개인정보 보호법을 위반하여 발생한 손해배상 책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다(제26조 제6항). 따라서 이 경우 개인정보처리자는 사용자 책임을 지게 된다. 그러므로 사용자로서 지휘, 감독의 의무를 다한 경우에는 개인정보처리자가 면책될 수도 있다.

나. 개인정보처리자의 정의가 매우 모호하여 엄밀하고 명확한 구별기준

우리 개인정보 보호 법제에 의하면 개인정보처리자는 '업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등'을 의미한다(제2조 제5호). 즉, '개인정보파일을 운용하기 위한 목적을 가지고 개인정보를 처리하는 자'이어야 한다. 여기에서 '누가 개인정보처리자인지?'를 판단하는 핵심적인 기준의 역할을 하는 것은 '운용하는 자'라는 개념인데, '운용'이라는 용어는 법률용어로 활용된 사례가 적어서 무엇을 운용으로 볼 것인지에 대한 구별기준이나 판단 사례가 거의 없는 모호한 개념이다. '운용'의 사전적 의미는 '무엇을 움직이게 하거나 부리어 쓰는 것'을 말하는데, 어느 정도로 개입을 하여야 개인정보파일을 운용하는 것으로 볼 것인지에 대한 판단 기준이 마련되어야 한다. 현재와 같은 모호한 기준을 가지고는 누구를 개인정보처리자로 볼 것인지를 명확하게 구별해 내기 곤란하다.

한편, 일본의 개인정보 보호법에서는 '개인정보취급사업자'가 우리나라 개인정보 보호법의 '개인정보처리자'와 같은 책임과 의무의 주체가 되는데, '개인정보취급사업자'란 '개인정보 데이터베이스 등을 사업용으로 이용하는 자'를 말한다고 정의하고

265) 제26조

있다(제2조 제5항)[266]. 일본의 개인정보 보호법과 비교해 보면, '이용하는 자'의 요건이 '개인정보파일을 운용하는 자'의 요건에 비하여 완화되어 있음을 알 수 있다.

반면, 유럽연합의 GDPR에서는 '컨트롤러'란 '단독으로 또는 타인과 공동으로 개인정보 처리의 목적과 수단을 결정하는 자연인이나 법인, 공공기관, 기구 또는 기타 단체'이다(제4조 (7)).

<표5-1> 우리나라, 일본, 유럽연합의 개인정보처리 주체에 대한 개념 정의

국 가	주 체	정 의	핵심 개념
우리나라	개인정보처리자	업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등	'운용'
일본	개인정보취급사업자	개인정보데이터베이스 등을 사업용으로 이용하는 자	'이용'
유럽연합	개인정보 컨트롤러	단독으로 또는 타인과 공동으로 개인정보 처리의 목적과 수단을 결정하는 자연인이나 법인, 공공기관, 기구 또는 기타 단체	'처리의 목적과 수단을 결정'

위에서 본 것처럼 우리나라, 일본, 유럽연합의 개인정보처리 주체에 대한 개념 정의를 비교해 보면, 우리나라의 개인정보처리자 개념은 '운용' 여부로 판단하는 것으로서, '이용'이나 '처리의 목적과 수단을 결정'하는지 여부로 판단하는 것보다 가장 엄격한 것으로 판단될 가능성이 높다. 특히 유럽연합의 경우는 어떤 경우에 '처리의 목적과 수단을 결정'하는 것으로 볼 것인지와 관련해서, '핵심적 요소'(Essential vs. non-essential means)를 결정하는 경우에는 부수적인 요소에 대한 결정은 위임될 수 있다는 등으로 해석[267]을 통해서 그 범위를 확장하고 있는 것과 비교해 본다면, '운용'의 개념을 넓히는 해석이나 이를 구체화 시키는 시행령 등이 제정되지 않는 한 '운용'의

266) 손형섭 외(2017), 일본의 개인정보보호 법제·정책 분석에 관한 연구, 개인정보보호위원회 용역보고서, p66.
267) EDPB(2020), op. cit., p13.

범위는 좁게 해석될 가능성이 매우 높다.

따라서 실질적으로는 개인정보 처리의 목적과 방법을 결정하는 지시자로서, 그로 인한 처리의 이익을 누리는 자임에도 불구하고 현재의 우리나라 개인정보 보호법의 해석에 의하면 개인정보 파일을 '운용하는 자'가 아니라고 판단되어 책임 주체에서 완전히 배제될 가능성이 있다. 그래서 배후에서 실질적인 결정권자로서 개인정보 처리의 목적과 방법을 결정하는 자는 개인정보 처리의 이익을 향수하면서도 책임과 의무를 완전히 면하는 반면, 그로부터 사실상의 실행 업무만을 수행하는 자가 책임과 의무를 모두 부담하게 되어 결과적으로 과징금이나 손해배상금 등 책임을 감당할 수도 없게 되는 일이 발생할 가능성도 크다.

따라서 이와 관련하여 우리나라의 개인정보 보호 법제에서도 GDPR의 해당 규정의 취지를 반영하여 개인정보 처리와 관련하여 책임과 의무의 토대인 개인정보처리자, 수탁처리자, 개인정보취급자의 개념을 재정비할 필요가 있다. 아울러 개인정보처리자의 개념은 개인정보의 개념과 마찬가지로 개인정보 보호법의 적용 범위를 결정하는 매우 중요한 개념임에도 불구하고[268], 그동안 개인정보처리자의 판단 기준을 구체화하려는 노력이 미비하였는데[269], 어떤 기준으로 개인정보처리자를 판단할 것인지에 대한 구체적인 기준도 마련할 필요가 있다. 이와 관련해서는 컨트롤러와 프로세서의 구별기준에 대해서 여러 의견서, 가이드라인 등을 마련하면서, 새로운 개인정보 처리의 유형에서는 어떻게 구별하고 적용할지를 계속해서 구체화해 나가고 있는 유럽연합의 노력과 성과를 검토하여 활용할 필요가 있다.

다. 현행 법제의 개인정보처리자, 수탁자, 취급자 구별

1) 위탁이라는 용어의 문제

우리나라 개인정보 보호 법제는 타인에게 개인정보를 처리하도록 맡기는 관계를 일괄

268) 우리 개인정보 보호법에서는 거의 대부분의 책임과 의무, 벌칙과 손해배상 책임 등의 규정이 개인정보처리자에게 부과되어 있고, 수탁처리자는 개인정보처리자에 대한 규정을 준용하고 있기 때문에 개인정보처리자나 수탁처리자가 아닌 자는 개인정보 보호법과 관련해서는 거의 아무런 책임도 지지 않는다.

269) 예를 들어, 그 동안 발간된 개인정보 보호법 해설서(행정안전부)에서도 개인정보처리자의 판단기준, '운용'의 판단기준 등에 대해서는 구체화된 내용이 없다.

하여 ‘위탁’이라고 표현하면서, ‘위탁’에 대해서는 별도의 개념 정의가 없다. 따라서 통상의 용례에 따라야 할 텐데, 개인정보의 처리를 맡기는 구체적인 법률관계가 매우 다양한데 이를 모두 일괄하여 ‘위탁’이라고 표현하는 것은 적절해 보이지는 않는다. ‘개인정보처리자를 대신하여 처리하는’과 같이 다양한 법률관계가 모두 포괄될 수 있는 표현을 사용하는 것이 혼란을 줄일 수 있을 것이다.

2) 개인정보처리 위탁자와 수탁자의 책임

우리 개인정보 보호 법제에 의하면 개인정보 처리의 위수탁 관계가 있는 경우에 수탁자가 아닌 위탁자에게 개인정보처리자로서의 법률상 책임이 존속하는지에 대해서는 명확한 규정은 두고 있지 않다. 개인정보 처리를 위탁할 경우 업무수탁자는 개인정보처리자의 일부 조항의 개인정보처리자의 책임과 의무가 준용된다는 규정이 있을 뿐인데[270], 개인정보처리자가 개인정보처리자로서의 책임을 면한다는 규정이 없기 때문에 수집 제한, 제공의 제한, 목적 외 이용의 제한, 개인정보의 파기 등과 같은 여러 가지 개인정보처리자의 책임과 의무는 여전히 준수해야 할 것이다.

수탁처리자가 준용 규정에 의해서 함께 부담할 의무는 개인정보 수집, 이용에 대한 개인정보 보호법 규정의 준수(제15조), 수집 제한(제16조), 제공의 제한(제17조), 목적 외 이용의 제한(제18조), 개인정보의 파기(제21조), 동의 방법(제22조), 민감정보의 처리 제한(제23조), 고유식별정보의 처리 제한(제24조), 영상정보처리기기의 설치, 운영(제25조), 개인정보취급자에 대한 감독(제28조), 가명정보 처리에 대한 의무(제28조의2 ~ 제28조의7), 개인정보의 안전조치 의무(제29조), 처리방침의 수립과 공개(제30조), 개인정보 보호책임자의 지정(제31조) 등은 물론, 개인정보 영향평가(제33조), 개인정보 유출통지(제34조), 과징금(제34조의 2), 개인정보의 열람(제35조), 정정, 삭제(제36조), 처리정지(제37조) 등이다.

3) 수탁자에 의한 손해발생 시의 개인정보처리 위탁자의 면책 허용규정의 문제

한편, 개인정보 보호법은 개인정보 수탁처리자를 손해배상 책임에 있어서 개인정보처리자의 소속 직원으로 본다(제26조 제6항)고 규정하고 있다. 이는 개인정보 처리의 위탁

270) 개인정보 보호법 제26조 제7항은 “수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.”고 규정하고 있다.

시 개인정보 처리의 위탁자를 사용자로 보고 수탁자를 피용자로 본다는 취지인데, 이는 개인정보 처리 위탁자에게 선임과 감독에 상당한 주의를 한 경우에는 면책을 허용하는 것이어서 책임의 원칙에 부합하는 것으로 보기 어렵다. 특히 개인정보 보호법이 개인정보의 처리와 관련한 처리자로서의 책임과 의무를 위탁자에게 부과하고 있는 상황에서 그 내부의 관계에 의하여 면책 여부가 결정될 수 있도록 사용자책임의 구조를 대입시키는 것은 부적절해 보인다. 민법의 사용자 책임 규정은 다음과 같다.

> 제756조(사용자의 배상책임) ① 타인을 사용하여 어느 사무에 종사하게 한 자는 피용자가 그 사무집행에 관하여 제삼자에게 가한 손해를 배상할 책임이 있다. 그러나 사용자가 피용자의 선임 및 그 사무감독에 상당한 주의를 한 때 또는 상당한 주의를 하여도 손해가 있을 경우에는 그러하지 아니하다.
> ② 사용자에 갈음하여 그 사무를 감독하는 자도 전항의 책임이 있다. <개정 2014. 12. 30.>
> ③ 전2항의 경우에 사용자 또는 감독자는 피용자에 대하여 구상권을 행사할 수 있다.

또한 사용자책임의 구조를 도입할 경우에는 수탁자가 사무집행의 범위를 넘는 불법행위를 하여 개인정보 침해가 발생하는 경우, 정보주체는 마땅히 책임을 물을 수 없게 될 수도 있다. 그리고 사용자책임의 구조를 도입할 경우에는 우리나라 법원이 택하고 있는 '피해자의 중대한 과실'이 있는 경우에도 개인정보처리자에게 면책을 인정하게 된다. 이것도 개인정보 보호법의 취지에 비추어 적절하다고 보기 어렵다[271].

라. 개인정보처리자와 수탁처리자의 책임

우리 개인정보 보호법에서는 개인정보 처리 업무를 위탁하는 것과 관련한 규정은 단 1개의 조문인데, 다음과 같은 내용을 포함한 문서로 해야 한다는 규정만 두고 있다[272].

---

271) 대법원 2003. 2. 11 선고, 2002다62029 판결.
"피용자의 불법행위가 외관상 사무집행의 범위 내에 속하는 것으로 보이는 경우에 있어서도, 피용자의 행위가 사용자나 사용자에 갈음하여 그 사무를 감독하는 자의 사무집행 행위에 해당하지 않음을 피해자 자신이 알았거나 또는 중대한 과실로 인하여 알지 못한 경우에는 사용자책임을 물을 수 없고, 사용자책임이 면책되는 피해자의 중대한 과실이라 함은 거래의 상대방이 조금만 주의를 기울였더라면 피용자의 행위가 그 직무권한 내에서 적법하게 행하여진 것이 아니라는 사정을 알 수 있었음에도 만연히 이를 직무권한 내의 행위라고 믿음으로써 일반인에게 요구되는 주의의무에 현저히 위반하는 것으로 거의 고의에 가까운 정도의 주의를 결여하고, 공평의 관점에서 상대방을 구태여 보호할 필요가 없다고 봄이 상당하다고 인정되는 상태를 말한다."

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 위탁업무의 목적 및 범위
4. 재위탁 제한에 관한 사항
5. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
6. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
7. 법 제26조제2항에 따른 수탁자(이하 "수탁자"라 한다)가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

이런 태도는 GDPR에서 개인정보 처리의 위수탁에 대하여 매우 엄격하고, 치밀한 규율을 하고 있는 것과 대비가 된다. 우리 개인정보 보호법에서도 위수탁 등 제3자에게 처리를 맡기는 경우에 대한 투명성 강화와 책임성 강화를 위한 상세한 규율을 신설하는 방향으로 법제 개선을 하는 것이 바람직할 것이다.

아울러 개인정보 보호법에서 정하고 있는 위탁처리에 관한 규정으로는 위탁사실 공지, 수탁자 교육과 감독의무가 있다. 그래서 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다[273]. 그리고 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 하고, 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 마찬가지이다[274].

한편, 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다는 의무를 부담한다[275].

4. 우리나라 개인정보 보호법의 개정 필요성과 방향

가. 개정 필요성

현행 우리나라 개인정보 보호 법제에서 개인정보처리자와 수탁자, 개인정보취급자, 제

272) 개인정보 보호법 제26조 제1항, 개인정보 보호법 시행령 제28조 제1항
273) 개인정보 보호법 제26조 제3항
274) 개인정보 보호법 제26조 제4항
275) 개인정보 보호법 제26조 제5항

3자로 나누고 있는데, 이를 실질적인 책임의 원칙에 부합하도록 정비하는 것이 바람직할 것이다. 아울러 개인정보 처리위탁과 관련해서도 처리를 맡기는 경우에 요건과 책임을 명확하게 하는 것이 필요하다.

나. 개인정보처리자 개념 명확화와 실질적 이득을 얻고 영향력을 행사하는 자 포함할 필요

GDPR은 컨트롤러와 프로세서, 공동 컨트롤러 개념을 정의하고, 그 구분기준을 구체화해 나가고 있는데, 이는 우리 개인정보 보호법에서도 수용할만한 점이다.

GDPR은 개인정보파일의 처리 목적과 방법을 결정하는 자를 컨트롤러로 보고, 실제로 그 자가 개인정보파일에 접근하거나, 해당 개인정보파일을 처리하지 않더라도 그에게 컨트롤러로서의 책임을 부과하고 있는데, 우리나라의 경우는 개인정보파일의 운용도 타인에게 지시하였다면 그 자는 개인정보처리자로 볼 수 없고, 해당 지시자는 개인정보 보호법과 관련해서는 어떤 의무도 부담하지 않게 되는데, 이는 오늘날 개인정보를 처리하는 업무를 전문으로 하는 서비스가 확산되는 현실에서 권한과 책임이 상응하는 것으로 보기 어렵다. 그래서 우리 법제에도 개인정보처리자의 개념을 명확하게 하고, 실질적으로 개인정보 처리에 대한 결정을 하는 자에 대해서도 책임을 부담할 수 있도록 처리자의 개념을 현재의 운용자보다는 완화하는 것이 바람직해 보인다.

아울러 처리자의 구별기준을 명확하게 하면서, 이를 현실에 부합하도록 끊임없이 구체화하는 노력이 이루어질 필요가 있다.

다. 공동처리자 개념 도입 필요

우리나라 법제에도 공동개인정보처리자라는 개념을 도입할 필요가 있다. 현행 법제상으로도 공동개인정보처리자가 인정되지 않는다고 보기는 어려울 수도 있지만, 공동개인정보처리자 개념을 도입하면서, 공동개인정보처리자 상호의 책임이나 역할 등을 명료하게 규율하고 정보주체에게 알리도록 하여 투명성과 책임성을 강화할 필요가 있다.

라. 개인정보 처리위탁 시의 책임성 강화 필요

우리나라 개인정보 보호법은 개인정보 처리위탁이라는 용어를 사용하고 있는데, 위탁의 정의가 명확하지 않아서 혼동을 초래한다. 따라서 용어를 명확하게 정리하는 것이 바람직해 보인다.

아울러 우리나라 개인정보 보호법은 GDPR과 달리 개인정보 처리자가 개인정보 처리를 위탁하는 경우의 요건과 절차 및 책임성과 투명성을 보장할 수 있는 규율이 매우 빈약하다. 따라서 우리나라 법제에도 개인정보를 대신 처리하도록 하는 경우의 요건과 절차 및 책임성과 투명성을 보장할 수 있는 규율을 신설할 필요가 있다.

우리나라 개인정보 보호법은 위탁 처리시의 손해배상 책임에 대하여 수탁자를 위탁자의 소속 직원으로 본다고 하여 사용자책임의 요건을 충족하는 경우에만 위탁자가 책임을 부담하는 것으로 규정하고 있다. 이런 태도는 GDPR이 컨트롤러에게 많은 책임을 부여하고 있는 것과 비교하여 개인정보 처리자의 책임을 지나치게 약화시키는 태도이다. 따라서 우리 법제에도 개인정보 처리위탁의 민사상 손해배상 책임에 대해서도 책임성을 강화하는 방향으로 개선할 필요가 있다.

제2절 안전조치를 취할 책임과 설명과 입증 의무

1. 개요

GDPR은 컨트롤러와 프로세서가 부담할 안전조치와 관련한 의무를 매우 상세하게 두고 있다. 포괄적인 안전조치 의무에 대한 규율(제24조)을 두고 있을 뿐만 아니라 설계에 의한 개인정보 보호와 기본설정을 통한 개인정보 보호 의무도 새롭게 도입하였다(제25조). 아울러 보안과 관련한 기술적, 조직적 조치에 포함되어야 할 의무의 내용을 보다 구체화하여 제시하고 있고(제32조), 고도의 위험이 예상되는 경우에는 개인정보보호 영향평가를 시행하여 기술적, 조직적 조치를 수립, 검토, 평가하도록 하고 있다(제35조). 이와 같은 조치들은 최신의 기술을 고려하도록 하고 있으며(제24조), 지속적, 주기적으로 검토, 평가하고 최신화하도록 하고 있다(제24조, 제25조, 제32조, 제35조).

이와 비교하여 우리나라의 개인정보 보호 법제는 개인정보처리자의 안전조치 의무에 대해서 20여년 전의 입법체계로서 분절적이고 매우 형식적인 수준에 머무르고 있다. 따라서 이와 같은 GDPR의 입법태도를 적극 수용하여, 안전조치와 관련된 규정을 대폭 수정하고 보완할 필요가 있다.

2. GDPR의 안전조치 의무

가. 포괄적인 기술적, 조직적 조치 의무

GDPR은 컨트롤러가 수행해야 하는 적절한 기술적, 조직적 조치의무를 제24조에서 매우 포괄적으로 규정하고 있다. 제24조는 GDPR이 적용되는 모든 컨트롤러에 대하여, 모든 개인정보 처리를 대상으로 규정하고 있다(24조 1항). 즉, 모든 컨트롤러는 GDPR이 적용되는 모든 개인정보 처리에서 기술적, 조직적 조치를 취해야 한다. 처리란 '개인정보 또는 개인정보 세트에 대해 수행되는 수집, 기록, 조직화, 구조화, 보관, 조정 또는 변경, 검색, 참고, 사용, 전송에 의한 공개, 전파 또는 그 밖에 사용 가능하도록 하는 것, 정렬 또는 조합, 제한, 삭제 또는 파괴 등, 자동화된 수단에 의한 것인지와 관계 없이 모든 작업 또는 작업 세트를 의미한다' 고 정의되어 있기 때문에, 모든 부문에서 적절한 기술적, 조직적 조치가 취해져야 하는 것이다. 이와 같은 개인정보 처리의 모든 과정에 대하여 법 준수를 보증할 수 있는 조직적, 관리적 조치를 취할 포괄적 의무를 부과한 것이다.

반면, 우리나라 개인정보 보호법에서는 "개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다" (개인정보 보호법 제29조)는 규정을 두고 있어서 일부의 영역에 한정하고 있다.

나. 설명과 입증(Accountability) 및 두 가지 유형의 기술적, 조직적 조치

GDPR은 컨트롤러에 대하여 법률의 준수에 대한 설명과 입증 의무를 도입하고 있다[276]. 이를 'Accountability' 라고 부르는데, 개인정보 처리의 원칙을 규정한 제5조 제2

276) 설명과 입증(Accountability)의 원칙은 오랜 역사를 가지고 있는 원칙인데 일찍이 2010년에

항에서도 이를 규정하고 있고, 컨트롤러의 조직적, 기술적 안전조치 의무를 규정하면서도 이를 명확하게 규정하고 있다(제24조).

설명과 입증(Accountability) 원칙은 1980년의 OECD의 프라이버시 가이드라인[277]에서도 채택된 것으로, APEC의 원칙, 캐나다의 공정한 개인정보처리의 원칙 등에서도 채택하고 있다[278]. Accountability[279]라는 용어는 앵글로-색슨의 용어로서, 책임을 어떻게 실행하고 있는지를 보여주고, 증명할 수 있도록 하는 것을 강조하는 용어로 인식되고 있다고 한다[280].

GDPR은 컨트롤러가 취해야 하는 기술적, 조직적 조치의 유형을 두 가지로 규정하고 있는데, 하나는 GDPR의 규정을 준수하여 개인정보 처리가 이루어질 수 있도록 보장할 수 있는 기술적, 조직적 조치이고, 다른 하나는 설명과 입증(Accountability)의 원칙에 따라서 신설된 내용으로, 개인정보 보호법을 준수하여 개인정보 처리가 이루어질 수 있도록 기술적, 조직적 조치를 취하고 있다는 것을 증명하고 설명할 수 있는 기술적, 조직적 조치이다. 전자는 법 준수 보장 조치이고, 후자는 입증 조치로 부를 수 있다.

특히, 후자와 관련해서 GDPR은 단순히 규정의 준수뿐만 아니라, 규정을 준수한다는 것을 입증할 수 있는 조치이어야 한다고 규정하고 있는데, 이는 단순한 입증책임의 전환뿐만 아니라, 프로세서가 적절한 수준의 기술적, 조직적 조치를 이행하여야 함은 물론, 규정 준수를 위한 적절한 기술적, 조직적 조치를 취한다는 것을 입증할 수 있는 수단까지도 포함되어야 함을 의미한다. 예를 들어 접근 통제를 하고 있다면 접근 통제를 하고 있다는 것을 입증할 수 있는 조직적 수단까지 마련해야 한다는 것이다. 이 점은 설명과

제29조 작업반은 이를 독립적인 규정으로 명확하게 규정하고 구체화해 나가야 한다는 취지의 의견을 제시하였었다. GDPR 제정 과정에서 그와 같은 의견이 받아들여져서 GDPR 제5조 제2항과 제24조에서 명확하게 설명과 입증(Accountability)의 원칙이 규정되게 된 것으로 볼 수 있다. Opinion 3/2010 on the principle of accountability, Towards a Proposal for a General Provision on Accountability, p8.

277) A data controller should be accountable for complying with measures which give effect to the [material] principles stated above.

278) ARTICLE 29 DATA PROTECTION WORKING PARTY(2010b), Opinion 3/2010 on the principle of accountability adopted on 13 July 2010, WP 173. pp6-7.

279) accountability라는 용어를 잘 설명할 수 있는 번역 용어를 찾기가 쉽지 않아서, reinforced responsibility, assurance, reliability, trustworthiness 프랑스어로는 obligation de rendre des comptes 등이 제시되기도 했다고 한다. implementation of data protection principles이라고도 한다. Ibid., p8.

280) Ibid., p7.

입증(Accountability)의 원칙을 도입하고 있지 않은 우리나라의 개인정보 보호 법제의 태도와는 다른 점이다.

규정 준수를 보증하는 조직적, 기술적 조치를 취하고 있다는 것을 입증할 수 있는 기술적, 조직적 조치가 취해져야하기 때문에 정보주체나 감독기관이나 개인정보 보호책임자는 언제든지 해당 기술적, 조직적 조치를 제시할 것을 요구할 수 있다. 이에 해당하는 조치 내용으로는 개인정보 처리에 대한 기록이나, 처리에 대한 평가 등이 될 수 있고, 승인된 행동강령(approved code of conduct)이나 승인된 인증 메커니즘을 준수하고 있다는 것은 컨트롤러의 의무 준수를 입증하는 요소로 사용될 수 있다(제24조 제3항).

다. 적절한 기술적, 조직적 조치의 판단 기준

GDPR은 적절한 기술적, 조직적 조치의 판단기준으로 '처리의 성격, 범위, 맥락 및 목적과 자연인의 권리와 자유에 대한 가능성과 심각성의 정도가 다양한 위험'을 고려하도록 하고 있다[281]. 이는 위험수준에 기반한 접근방법이다.

라. 필요시 검토 및 갱신

한편, GDPR은 적절한 기술적, 조직적 조치가 필요시 검토 및 갱신되어야 한다는 점도 분명하게 규정하고 있다. 검토와 갱신을 해야 할 시기인 '필요시'라는 것은 GDPR이 판단기준으로 제시한 요소인 '처리의 성격, 범위, 맥락 및 목적과 자연인의 권리와 자유에 대한 가능성과 심각성의 정도가 다양한 위험'에 변화가 생길 때를 의미한다. 이때마다 검토와 갱신이 이루어져야 한다[282]. 아울러 해당 조치는 지속적으로 재검토가 되고 갱신되어야 한다. 기술적, 조직적 조치는 제25조의 설계를 통한 개인정보 보호와 기본설정을 통한 개인정보 보호와 결합한다.

한편, 자율 인증 메커니즘과 승인된 행동강령을 준수하는 것이 의무 준수를 입증하는 요소로 사용될 수 있다고 규정하여, 자율 인증 메커니즘과 승인된 행동강령의 준수를 위한 기술적, 조직적 조치도 컨트롤러의 책임으로 하고 있다. 따라서 이를 통해서 기술적,

281) 제24조 제1항
282) 제24조 제1항

조직적 조치가 무엇일지가 계속 구체화될 수 있을 것이다.

이와 같은 기술적, 조직적 조치를 취할 것을 컨트롤러의 책임으로 함으로써 법률 준수를 위해 필요한 적절한 조치를 하지 않는 것에 대해서 책임을 추궁할 수 있게 되고, 이는 사전 예방적인 역할을 하게 될 것이다.

반면, 우리나라의 경우는 법 준수를 위해 모든 처리에 대해서 기술적, 조직적 조치를 취할 의무가 없고, 분실, 유출을 방지하기 위한 조치만을 규정하고 있어서, 그 외의 영역에서는 기술적, 조직적 조치를 취하지 않은 것을 문제 삼을 수는 없고, 결과 발생에 대해서만 문제를 삼을 수 있을 뿐이다. 따라서 사전 예방적인 조치를 취하도록 하는 역할이 제한된다. 아울러 설명과 입증의 책임에 대한 규정도 없다.

3. 우리나라 개인정보 보호법의 규정과 개선방안

가. 포괄적인 기술적, 조직적 조치 의무에 대한 법률규정이 미비함

우리나라 개인정보 보호법에서도 개인정보처리자에게 기술적, 조직적 조치를 취할 의무를 부과하는 규정이 있는데(개인정보 보호법 제29조), '개인정보의 분실, 도난, 유출, 위조, 변조 또는 훼손되지 아니하도록' 조치를 취할 의무를 진다고 하여, 기술적, 조직적 조치 의무의 범위가 '분실, 도난, 유출, 위조, 변조 또는 훼손되지 아니하도록' 하는 것에 국한되는 것으로 오인될 가능성이 있다. 이 규정은 보안과 관련된 것으로, GDPR에서는 제32조의 처리 보안에 관한 조항에 상응하는 것이다. 이와 같은 개인정보 보호법의 규정에 의할 경우에는 예를 들어 최소수집의 원칙을 준수하기 위한 조치, 내부 직원에 의한 활용을 막기 위한 조치 등은 안전조치로서 포함되어 있지 않다. 즉, 분실, 도난, 유출, 위변조나 훼손이 아니면 안전조치 의무가 없는 것이다.

그래서 예를 들어 최소수집의 원칙을 준수하기 위한 조치를 취하지 않고 있는 경우, 개인정보 보호법은 그로 인하여 과다수집이 되었거나, 내부 직원에 의한 활용을 막기 위한 안전조치를 취하지 않는 경우 그로 인하여 내부 직원의 악용이 있을 경우에만 문제가 된다. 그러나 GDPR에서는 그 자체가 안전조치 위반이 되고 시정의 대상이 될 수 있다. 물론, 개인정보 보호법 시행령과 개인정보 보호위원회 고시에서는 제29조의 조직적, 기술적 조치가 단지 보안에 관한 것만이 아닐 수 있다고 유추할 수 있는 내용도 포함되

어 있지만 이는 고시의 규정에 불과하기 때문에, 개인정보 보호법에서 명확하게 모든 개인정보 처리에 대하여 안전조치 의무가 있다는 내용이 포함되도록 하는 것이 바람직할 것이다.

나. 포괄적인 이행 수단의 규정 필요

개인정보 보호법은 내부 관리계획 수립, 접속기록 보관 등을 열거하면서, 대통령령으로 안전성 확보에 필요한 기술적, 관리적, 물리적 조치를 두도록 하고 있다. 그에 따라 시행령은 내부 관리계획의 수립 및 시행, 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치, 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치, 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조, 변조 방지를 위한 조치, 개인정보에 대한 보안프로그램의 설치 및 갱신, 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치를 들고, 세부기준을 개인정보 보호위원회가 고시한다고 하였다[283]. 물론, 개인정보 보호위원회는 열거된 조치에 대해서 '최소한의 기준'이라고 규정하고 있지만, 열거된 항목 자체가 최소한의 기준이라는 것인지 아니면 열거된 항목에 따른 규율된 내용이 최소한의 기준이라는 것인지도 논란의 여지가 있다. 실질적으로는 열거된 조치에 준하는 책임을 다하면 보호 의무를 다한 것으로 해석될 소지가 충분하다.

따라서 오해의 소지를 없앨 수 있도록, 안전조치의 범위를 포괄적으로 표시하고, 기술적, 조직적 조치의 범주와 내용도 그에 부합하도록 수정할 필요가 있다.

다. 두 가지 유형의 기술적, 조직적 조치를 명시할 필요

GDPR은 컨트롤러가 취해야 하는 기술적, 조직적 조치의 유형을 두 가지로 규정하면서, 규정을 준수하여 개인정보 처리가 이루어질 수 있도록 기술적, 조직적 조치를 취하고 있다는 것을 증명할 수 있는 기술적, 조직적 조치도 아울러 채택하도록 하고 있다. 이는 단순한 입증책임의 전환뿐만 아니라, 규정 준수를 위한 적절한 기술적, 조직적 조

283) 규정을 보면, 부정이용, 부정접속, 부정제공, 식별화로 인한 개인식별, 개인추적, 평가 등의 권리 침해 등이 명시되지 않고 있다.

치를 취한다는 것을 입증할 수 있는 수단까지도 포함하도록 하여, 투명성 강화와 책임성 강화는 물론 개인정보주체의 권리 행사를 위해서도 매우 효과적인 규정이다.

우리 법제에도 설명 및 입증의무(accountability)를 도입하여, 법률 준수를 위해 적절한 기술적, 조직적 조치를 취하고 있다는 것을 입증할 수 있는 조치를 취할 의무를 도입하는 것이 바람직할 것이다.

이 규정이 도입된다면, 정보주체나 개인정보 보호위원회, 개인정보 보호책임자가 적정한 경우 해당 기술적, 조직적 조치를 제시할 것을 요구할 수 있게 될 것이다. 이에 해당하는 조치로는 개인정보 처리에 대한 기록이나, 처리에 대한 평가 등이 될 수 있고, 승인된 행동강령이나 승인된 인증 메커니즘을 준수하고 있다는 것은 컨트롤러의 의무 준수를 입증하는 요소로 사용될 수 있기 때문에, 행동강령이나 인증 메커니즘의 도입과 활성화에도 기여할 것이다.

라. 적절한 기술적, 조직적 조치의 판단 기준 명시

우리 법제에도 적절한 기술적, 조직적 조치의 판단기준을 '처리의 성격, 범위, 맥락 및 목적과 자연인의 권리와 자유에 대한 가능성과 심각성의 정도가 다양한 위험'을 고려한다는 점을 분명하게 규정하여 위험수준에 기반한 접근방법을 명시하는 것이 바람직할 것이다.

마. 필요시 검토 및 갱신 규정 도입

우리 법제에도 GDPR과 같이 적절한 기술적, 조직적 조치를 필요시 검토하고 갱신되어야 한다는 점을 분명하게 규정할 필요가 있다. 이와 관련하여 검토와 갱신을 해야 할 시기인 '필요시'가 '처리의 성격, 범위, 맥락 및 목적과 자연인의 권리와 자유에 대한 가능성과 심각성의 정도가 다양한 위험'에 변화가 생길 때를 의미한다는 것도 분명하게 하는 것이 바람직하다. 이와 같은 조치는 지속적으로 재검토가 되고 갱신되어야 한다.

만약 설계를 통한 개인정보 보호와 기본설정을 통한 개인정보 보호 제도를 새로 도입한다면, 이와 결합하여 안전조치 의무가 내실 있게 유지될 수 있을 것이다. 그리고 자율인증 메커니즘과 승인된 행동강령도 활성화한다면, 해당 기술적, 조직적 조치가 지속적

으로 구체화될 수 있을 것이다.

제3절 개인정보 처리의 보안에 관한 규정

1. 개요

개인정보 처리의 보안에 관한 규정도 유럽연합의 GDPR에서는 독특한 원칙과 기준에 입각하여 상세한 규정을 두고 있는데 우리나라 개인정보 보호법에도 도입하는 것이 바람직할 것이다.

GDPR은 컨트롤러와 프로세서에 대하여 개인정보 처리 보안에 관한 규정을 두면서 최신 기술 등을 고려한 위험기반 접근법에 의하여 보안조치를 두도록 하고 있고, 효율성을 지속적으로 평가하도록 하고 있으며, 기술 중립성을 유지하고 있다. 이와 같은 GDPR의 태도는 개인정보 처리가 야기하는 위험의 수준에 맞추고, 기술의 발전에 맞추어 지속적으로 그에 상응하는 보안 조치를 취하도록 하기 위함이다.

반면 우리나라 개인정보 보호법은 매우 형식적인 조치를 명문화함으로 인해서 그 동안에도 해당 규정이 오히려 개인정보 보호의 한계로 작용하고, 면책의 근거로 활용되고 있다는 비판이 있어 왔다. 그런 점에서 우리 개인정보 보호법에서도 GDPR에서 채택하고 있는 원칙과 방법에 대한 입법태도를 적극 수용할 필요가 있다.

2. GDPR의 규정

가. GDPR의 개인정보 처리의 보안에 관한 규정

GDPR은 개인정보의 처리와 관련한 보안에 대하여 위험에 대한 적절한 수준의 보안을 보장하기 위해 적절한 기술적, 조직적 조치를 이행할 의무가 있다는 점을 명시하고 있다. GDPR은 그 판단 기준으로 최신 기술, 실행 비용, 처리의 성격, 범위, 맥락 및 목적, 그리고 처리가 자연인의 권리와 자유에 대해 갖는 가능성과 심각성의 정도가 다양한 위험을 고려하도록 하고 있다. 이와 관련하여 '통상의 기술'이 아닌 '최신 기술'을 고려하도록 한 것은 큰 의미가 있다[284].

나. 적절한 수준의 보안을 보장하기 위한 적절한 기술적, 조직적 조치

GDPR은 개인정보의 처리와 관련하여 위험에 대한 적절한 수준의 보안을 보장하기 위한 적절한 기술적, 조직적 조치를 이행해야 한다고 포괄적으로 규율하면서, 보안조치의 예시를 들고 있는데, 그 내용은 다음과 같다[285].

첫째, 개인정보의 가명화와 암호화를 들고 있다. 개인정보의 가명화와 암호화는 중요한 보안조치의 일환인 것이다.

둘째, 처리 시스템 및 서비스의 지속적인 기밀성, 무결성, 가용성 및 복원력을 보장하는 능력이다. 처리 시스템과 서비스의 기밀성을 보장한다는 것은 공개됨으로 인해서 발생하는 문제를 방지하기 위한 수단을 갖추어야 한다는 것이다. 무결성이란 부정한 수정이나 삭제 등을 방지하기 위한 수단을 갖추어야 한다는 것이다. 가용성이란 허가받지 않거나 우발적인 손실이나 파괴를 방지하기 위한 수단을 갖추어야 한다는 것이다.

셋째, 물리적 또는 기술적 사고가 발생했을 경우 적시에 개인정보의 가용성과 접근성을 복원하는 능력을 들고 있다.

넷째, 처리 보안을 보장하기 위한 기술적, 조직적 조치의 효과를 정기적으로 시험, 평가, 감정하는 절차를 들고 있다.

한편, GDPR은 특히 컨트롤러와 프로세서의 권한에 따라 행위하는 자가 개인정보를 처리할 때, 컨트롤러의 지시에 의한 경우 외에는 정보를 처리하지 않도록 하기 위한 조치를 취하도록 의무를 부과하고 있다.

이와 같은 보안조치의 특징은 다음과 같다.

첫째, 포괄성이다. 프로세서와 컨트롤러 모두에게 적용되며, 위험이 있을 경우 이를 완화시키기 위한 조치가 필요하다는 것이다. 그리고 기밀성, 무결성, 가용성과 복원성을 보장하기 위한 모든 기술적, 조직적 수단을 포괄하는 것이다.

둘째, 기술중립성이다. GDPR은 위와 관련하여 어떤 특정한 기술을 제시하지 않는다.

셋째, 해당 기술적 수단은 최신기술의 수준에 조응해야 하고, 해당 수단의 적정성을 시험, 평가, 감정하는 절차를 갖추어 라이프 사이클 동안 적절성을 유지할 수 있도록 하고 있다.

---

284) 제32조 제1항
285) 제32조 제1항의 (a) ~ (d)

다. 보안조치의 적절성 평가 기준

GDPR은 보안 수준의 적절성을 평가할 때 최신 기술, 실행 비용, 처리의 성격, 범위, 맥락 및 목적, 그리고 처리가 자연인의 권리와 자유에 대해 갖는 가능성과 심각성의 정도와 다양한 위험을 고려하도록 하고 있다[286]. 이는 위험기반 접근법이라고 볼 수 있다. 아울러 GDPR은 전송 또는 보관되거나 달리 처리되는 개인정보의 우발적 또는 불법적 파괴, 손실, 변경, 무단 공개나 그에 대한 접근 등 개인정보 처리에서 드러나는 위험이 특히 고려되어야 한다고 규정하고 있다[287].

라. 승인된 행동강령이나 승인된 인증 메커니즘의 활용

GDPR은 승인된 행동강령이나 승인된 인증 메커니즘을 준수하는 것이 보안에 대한 적절한 기술적, 조직적 조치를 취한 것임을 입증하는 요소로 사용될 수 있다는 점도 규정하고 있다. 감독기구는 행동강령이나 인증 메커니즘을 인증할 경우, 해당 요소를 평가하여 승인을 할 것이다.

마. 접근제한

GDPR은 특히 컨트롤러와 프로세서가 컨트롤러나 프로세서의 권한에 따라 행위하는 자연인의 경우에는, 개인정보에 대한 접근권을 가진 사람이 컨트롤러의 지시에 의한 경우 외에는 그러한 정보를 처리하지 않도록 하기 위한 조치를 취해야 한다는 점을 별도로 명시하고 있다. 이는 접근통제를 분명하게 해야 한다는 것이다.

---

286) 제32조 제1항
287) 제32조 제2항

3. 우리나라 개인정보 보호법의 규정

가. 개인정보 보호법의 법률 규정

개인정보 보호법에서도 개인정보처리자의 안전조치에 대한 의무를 규정하고 있는데, 앞에서도 본 것처럼 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다고 규정하고 있고[288], 그에 대한 사항은 시행령 제30조, 개인정보 보호위원회의 고시를 두고 있다.

나. 조치의 이행 책임을 지는 범위와 이행수단

개인정보 보호법 제29조는 '개인정보의 분실, 도난, 유출, 위조, 변조 또는 훼손되지 아니하도록' 조치를 취할 의무를 진다고 안전조치의무의 범위를 규정하고 있고, 구체적인 이행수단으로 내부 관리계획 수립, 접속기록 보관 등과 대통령령으로 규정하는 안전성 확보에 필요한 기술적, 관리적, 물리적 조치가 있다. 시행령은 내부 관리계획의 수립 및 시행, 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치, 개인정보를 안전하게 저장, 전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치, 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조, 변조 방지를 위한 조치, 개인정보에 대한 보안프로그램의 설치 및 갱신, 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치를 들고, 세부기준을 개인정보 보호위원회가 고시한다고 하였다[289]. 고시한 세부기준과 관련하여 개인정보 보호위원회는 해당 열거하는 조치가 '최소한의 기준'이라고 규정하고 있지만, 열거된 조치에 준하는 책임을 다하면 보호의무를 다한 것으로 해석될 소지가 있다. 따라서 오해의 소지를 없앨 수 있도록, 안전조치의 범위를 포괄적으로 표시하고, 기술적, 조직적 조치의 범주와 내용도 대폭 수정할 필요가 있다.

---

288) 개인정보 보호법 제29조

289) 규정을 보면, 부정이용, 부정접속, 부정제공, 식별화로 인한 개인식별, 개인추적, 평가 등의 권리 침해 등이 명시되지 않고 있다.

다. 개인정보 안전조치 의무에 대한 현행 규정의 문제점

그동안 개인정보 보호법의 개인정보 안전조치 의무와 관련된 규정은 개인정보처리자의 책임을 제한하고, 개인정보 보호를 위한 다양한 조치의 범위를 축소하고, 처리자의 개인정보 보호에 대한 투자와 역할을 제한하는 역할을 해온 측면도 있었음을 부정할 수 없다. 실제로 안전조치의무에 규정되어 있지 않았기 때문에 책임이 없다거나, 안전조치 의무에 규정된 수준을 이행하였기 때문에 책임이 없다는 판결이 내려지기도 했다.

예를 들어 대법원[290]은 해킹프로그램을 이용하여 KT의 고객정보를 저장한 데이터베이스에 침입해, 2012. 2. 20.부터 2012. 7. 13.까지 피고 고객의 개인정보(주민등록번호, 휴대전화번호, 주소 등) 1,000만 건 이상을 위법하게 취득·유출하여, 유출된 고객들이 KT를 상대로 제기한 손해배상 청구소송에서 다음과 같이 피고 KT의 책임을 부인하였다.

"정보통신서비스 제공자가 위와 같은 법률상 또는 계약상 의무를 위반하였는지는, 해킹 등 침해사고 당시 일반적으로 알려져 있는 정보보안 기술 수준, 정보통신서비스 제공자의 업종과 영업 규모, 정보통신서비스 제공자가 취하고 있던 전체적인 보안조치의 내용, 정보보안조치에 필요한 경제적 비용 및 그 효용의 정도, 해킹기술 수준과 정보보안 기술 발전 정도에 따른 피해 발생 회피 가능성, 정보통신서비스 제공자가 수집한 개인정보의 내용과 개인정보 누출로 인하여 이용자가 입게 되는 피해 정도 등의 사정을 고려하여, 정보통신서비스 제공자가 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 등을 종합하여 판단해야 한다. 별도의 인증 서버를 둔 피고의 접근통제시스템 자체가 불완전하다거나, 피고가 개인정보 등 송·수신시 암호화 의무를 위반하였다고 볼 수 없다. 피고가 2011. 10. 11. 퇴직자 이○○의 전산영업시스템(N-STEP 시스템) ID를 폐기하였을 뿐만 아니라, 최○○이 그 이전에 이미 인증 서버를 우회하는 방법을 찾아낸 사실에 비추어 보면, 위 계정 폐기 여부와 이 사건 정보유출 사고 사이에 인과관계도 인정하기 어렵다. 따라서 피고가 퇴직자 이○○의 개인정보처리 시스템에 대한 접근권한을 말소하지 않았다거나, 그로 인하여 이 사건 정보유출 사고가 발생했다고 볼 수 없다. (적어도 국내에서는 이 사건 정보유출 사고와 같이 인증 서버를 우회하는 방식의 해킹이 성공한 적이 없었던 상황에서) 피고가 인증 서버에 저장된 접속기록을 확

290) 대법원 2017다207994, 2017다256910 판결.

인·감독한 이상 개인정보처리 시스템의 개인정보 처리 내역 등에 관한 확인·감독을 게을리 하였다고 보기 어렵다.”

예를 들어, 안전조치의무 중에는 10만 이상 접속자의 망 분리 의무와 주민등록번호 암호화 의무 등 도식화된 의무가 존재하는데, 이는 10만 미만인 경우는 오히려 망 분리 의무가 없다거나, 주민등록번호 외에는 암호화 의무가 없는 것으로 잘못 해석될 소지도 다분한 것이다. 게다가 안전조치의무가 파편화되어 있고 단순화되어 있어서 오히려 개인정보처리 기업에서 해당 항목 외의 개인정보 보호를 위한 기술 도입이나 시스템 구축, 조직적 체계 마련을 위한 노력을 기울이지 않게 하는 부작용도 있었다. 특히 최신 기술의 도입과 관련해서 해당 의무가 명시되어 있지 않고, 가명화 등의 새로운 기술의 적극적인 도입 등도 필요한데 이를 포괄하지 못하고 있다. 안전조치 의무 규정을 대폭 개선할 필요가 있다.

4. 개선방안

우리나라의 경우도 개인정보 보호법에서 개인정보 보호법을 준수하여 개인정보의 처리가 될 수 있도록 처리의 모든 영역에서 보안과 관련된 안전조치를 취할 책임이 처리자에게 있다는 것을 명시하는 것이 바람직할 것이다.

그 내용으로는 위험에 대한 적절한 수준의 보안을 보장하기 위해 적절한 기술적, 조직적 조치를 이행할 의무가 있다는 점을 명시하여 위험기반 접근을 도입하는 것이 바람직할 것이다. 아울러 판단기준에는 최신 기술, 실행 비용, 처리의 성격, 범위, 맥락 및 목적, 그리고 처리가 자연인의 권리와 자유에 대해 갖는 가능성과 심각성의 정도가 다양한 위험을 고려하도록 하는 것이 좋을 것이다. 아울러 전송 또는 보관되거나 달리 처리되는 개인정보의 우발적 또는 불법적 파괴, 손실, 변경, 무단 공개나 그에 대한 접근 등 개인정보 처리에서 드러나는 위험이 특히 고려되어야 한다고 규정하는 것이 바람직할 것이다.

적절한 수준의 보안을 보장하기 위한 적절한 기술적, 조직적 초치의 내용도 범주별로 구체화할 수 있다. 즉, 그 예시로는 개인정보의 가명화와 암호화, 처리 시스템 및 서비스의 지속적인 기밀성, 무결성, 가용성 및 복원력을 보장하는 능력, 물리적 또는 기술적 사

고가 발생했을 경우 적시에 개인정보의 가용성과 접근성을 복원하는 능력, 처리 보안을 보장하기 위한 기술적, 조직적 조치의 효과를 정기적으로 시험, 평가, 감정하는 절차를 둘 필요가 있다. 그리고 승인된 행동강령이나 승인된 인증 메커니즘을 준수하는 것이 보안에 대한 적절한 기술적, 조직적 조치를 취한 것임을 입증하는 요소로 사용될 수 있다는 점도 규정하면 좋을 것이다.

제4절 설계에 의한 개인정보 보호와 기본설정에 의한 개인정보 보호

1. 개요

설계에 의한 프라이버시 보호(Privacy by design) 또는 설계에 의한 개인정보 보호라는 개념은 IT 시스템이나, 네트워크 기반, 사업 수행 등에서 프라이버시 보호나 개인정보 보호를 사전적으로 내재하도록 한다는 관념에 기반한 것이다. 이 개념은 캐나다 온타리오의 개인정보 보호 감독관이던 앤 카부키안(Ann Cavoukian)에 의해 최초로 제안되었고[291], 1995년에 '프라이버시 보호 기술에 대한 공동 보고서'에서 처음으로 공식화되었다[292]. 그 후 캐나다의 개인정보 보호원칙, 호주의 원칙, APEC의 원칙 등에서 수용되었고, FTC의 보고서 등에서도 수용되었다.

GDPR은 '설계에 의한 개인정보 보호'와 '기본설정에 의한 개인정보 보호' 규정을 새롭게 컨트롤러의 의무로 도입하였다(제25조). 이 규정은 개인정보 처리가 있는 경우에는 개인정보 보호를 설계 단계에서부터 고려하고, 기본설정에서 개인정보 보호를 의무화하는 내용으로 구성하였다. 특히 GDPR은 해당 조치와 관련하여 통상의 기술이 아니라 최신

291) 7가지 기본원칙을 다음과 같이 제시하고 있다. 1. Proactive not reactive; preventative not remedial. 2. Lead with privacy as the default setting. 3. Embed privacy into design. 4. Retain full functionality (positive-sum, not zero-sum). 5. Ensure end-to-end security (Full Lifecycle Protection) 6. Maintain visibility and transparency – Keep it open. 7. Respect for user privacy – keep it user-centric.

292) Privacy Enhancing Technologies: the path to anonymity.. 캐나다 온타리오 개인정보감독기구(the Information and Privacy Commissioner of Ontario)와 네덜란드 개인정보 감독기구(Dutch Data Protection Authority), 네덜란드 응용과학연구기구(Netherlands Organisation for Applied Scientific Research)의 공동 보고서.

기술을 고려하도록 하고, 처리가 자연인의 권리와 자유에 대해 갖는 가능성과 심각성의 정도가 다양한 위험을 고려하도록 하여 위험 기반 접근(risk-based approach)을 하도록 하였다[293]. 아울러 개인정보를 처리하는 애플리케이션 및 서비스는 물론이고, 제품에 대해서도 그 적용범위가 될 수 있음을 규정하였고, 단계에서도 개발, 설계, 선정, 사용할 때를 모두 대상으로 하였고, 공개 입찰의 맥락에서도 고려되어야 한다고 범위를 확장하고 있다[294]. 그리고 인증 메커니즘에도 이를 포함하도록 하고, 제24조와 결합하여 안전조치의 통합, 진화, 지속적인 점검을 하도록 하고 있다.

따라서 향후 이 규정은 제품의 설계, 선정, 사용, 공개 입찰 등에서 개인정보 보호원칙을 구체화할 수 있는 다양한 기준과 지침을 만드는 근거규정으로 발전해 나갈 것으로 보인다. 우리나라 개인정보 보호법에서는 이와 관련한 규정이 아직 도입되어 있지 않은데, 우리 법제에도 이를 도입할 필요가 있다.

2. GDPR의 규정

가. 설계에 의한 개인정보 보호

1) 대상 범위

GDPR은 설계에 의한 개인정보 보호와 기본설정에 의한 개인정보 보호를 적용할 범위로 자연인의 개인정보를 처리하는 애플리케이션, 서비스는 물론이고, 제품까지도 포함한다고 규정하고 있다[295]. 그리고 이들을 개발, 설계, 선정, 사용할 경우를 모두 해당 원칙을 적용할 대상으로 규율하였다[296]. 해당 제품, 서비스, 애플리케이션의 생산자는 그러한 제품, 서비스, 애플리케이션을 개발 및 설계할 때 개인정보 보호에 대한 권리를 고려하도록 권장되어야 하며, 최신 기술을 충분히 고려하여 컨트롤러와 프로세서가 개인정보 보호 의무를 충족할 수 있게 하도록 권장되어야 한다고 규정하고 있다. 한편, 이 원칙은 공개 입찰의 맥락에서도 고려되어야 한다고 규정하고 있다[297].

---

293) 제25조 제1항, 전문 78
294) 전문 78
295) 이것은 GDPR의 전문 78에서 규정하고 있는 것이어서 본문의 제25조에서는 해당 표현이 없다.
296) 전문 78

2) 고려할 사항

개인정보 보호 설계를 할 때 고려할 사항에는 최신 기술, 실행 비용, 처리의 성격, 범위, 맥락 및 목적, 그리고 처리가 자연인의 권리와 자유에 대해 갖는 가능성과 심각성의 정도가 다양한 위험을 고려하도록 했다[298].

여기서 '통상의 기술'이 아니라 '최신 기술'을 고려하도록 하고 있는 것은 큰 의미가 있다. 이는 실행 비용을 고려해야 하겠지만, 항상 최신 기술을 지속적으로 보완, 업데이트하도록 규정한 것이다. 아울러 GDPR은 위험 기반 접근법을 채택하고 있다. 그래서 해당 개인정보의 처리가 자연인의 권리와 자유에 중대한 영향을 미칠 수 있는 것일수록 기술적, 조직적 보호조치는 더 엄격하게 설계하도록 하고 있다.

3) 포함될 내용

설계에 포함되어야 하는 것은 GDPR에서 요구하는 모든 사항을 준수해야 하고, 정보주체의 권리를 보호해야 한다. 해당 기술적, 조직적 조치는 정보 최소화 등 개인정보 보호 원칙을 효과적인 방식으로 구현하고 필요한 보호조치를 처리에 통합하도록 설계해야 하며, 여기에는 가명화 같은 조치도 포함된다[299].

개인정보 처리의 원칙은 '적법성, 공정성, 투명성'(적법하게, 공정하게, 그리고 정보주체와 관련하여 투명한 방식으로 처리되어야 한다), '목적 제한'(구체적이고 명시적이며 정당한 목적으로 수집되어야 하고, 그러한 목적과 양립 불가능한 방식으로 추가 처리되어서는 안 된다. 공익을 위한 자료 보존 목적, 과학 또는 역사 연구 목적이나 통계 목적을 위한 추가처리는 원래 목적과 양립 불가능한 것으로 간주되지 않는다). '정보 최소화'(처리 목적과 관련하여 적절하고 관련성이 있어야 하며, 이에 따라 필요한 범위로 제한되어야 한다), '정확성'(정확해야 하며 필요한 경우 최신상태로 유지되어야 한다. 부정확한 개인정보가 처리 목적을 고려하여 지연 없이 삭제 또는 수정되도록 모든 합리적 조치를 취해야 한다), '보관 제한'(처리 목적에 필요한 기간보다 오래 정보 주체 식별을 허용하는 형태로 보관되어서는 안 된다. 개인정보가 공익을 위한 자료 보존 목적,

297) 전문 78
298) 제25조 제1항
299) 제25조 제1항

과학 또는 역사 연구 목적이나 통계 목적을 위해서만 처리되는 경우, 정보주체의 권리와 자유를 보호하기 위해 본 규정이 요구하는 적절한 기술적, 조직적 조치를 이행하는 조건으로 개인정보를 더 오래 보관할 수 있다.), ‘무결성과 기밀성’(적절한 기술적, 조직적 조치를 활용해 무단 또는 불법 처리와 우발적 손실, 파괴, 손상을 막는 등 개인정보의 적절한 보안을 보장하는 방식으로 처리되어야 한다), ‘책임성’(정보 컨트롤러는 이러한 점을 준수할 책임이 있으며, 이를 입증할 수 있어야 한다) 등이다. 따라서 이러한 개인정보 처리의 모든 원칙을 효과적으로 구현할 수 있도록 필요한 보호조치가 개인정보 처리에 통합되도록 설계되어야 한다.

4) 처리에 통합된 조직적, 기술적 조치의 적절성 판단 시점

설계를 통해서 처리에 통합된 조직적, 기술적 조치의 적절성을 판단하는 시점은 처리 수단 결정 시점과 실제 처리 시점이다[300]. GDPR에서 처리가 의미하는 것은 포괄적이기 때문에 수집, 보유, 검색 등이 이루어지는 모든 순간이 처리의 시점이다. 따라서 이것은 현재와 미래의 시점에서 계속적으로 적정성이 판단되어야 하며, 지속적인 업데이트가 이루어져야 함을 의미한다.

5) 인증 메커니즘의 역할

GDPR은 설계에 의한 개인정보 보호를 준수하는 하나의 방안으로 인증 메커니즘을 들고 있다. 인증 메커니즘은 자율규제의 일환으로, 개인정보 감독기관이 특정 부문의 개인정보처리자가 제정한 행동강령이 개인정보 보호 법제에 부합하는지를 검토하여, 승인하고, 해당 승인된 행동강령을 독립성을 가진 인증 모니터링 기구가 해당 개인정보처리자가 준수하는지 여부를 평가하고 지속적으로 확인하는 절차이다. 따라서 개인정보 감독기관은 인증 시에 해당 인증 메커니즘이 설계에 의한 개인정보 보호를 준수하는지를 검토하여 승인하는 과정을 통해서 구체화시킬 수 있을 것이다.

300) 제25조 제1항

나. 기본설정에 의한 개인정보 보호

1) 기본설정 의무

GDPR은 기본설정에 의한 개인정보 보호를 도입하였다. 이는 컨트롤러가 기본설정에서 개인정보 처리가 특정 목적 각각에 필요한 개인정보만 처리되도록 보장한다는 것이다. 이를 위해서 수집되는 개인정보의 양, 처리의 범위, 보관의 범위와 해당 정보에 접근할 수 있는 자의 범위가 특정 목적에 필요한 처리로 보장될 수 있도록 기본설정을 해야 한다[301]. 그 보장은 기술적, 조직적 조치를 포함한다. 즉, 개인정보가 특정 목적으로 최소한으로 처리될 수 있도록 기본설정을 하고, 통합하는 것이나 다른 목적을 위해 제공되는 것은 당사자의 동의를 얻어서 처리될 수 있도록 해야 한다는 것이다. 이는 개인정보 최소수집의 원칙을 보장하는 방안의 하나이다.

2) 접근 제한

특히 GDPR은 기본설정을 통해 개인정보가 개인의 개입 없이 무제한 수의 자연인이 접근 가능하게 되지 않도록 보장해야 한다는 규정을 두고 있다. 이는 인터넷의 정보처리와 관련된 것이다. 개인의 개입이란 해당 정보주체가 무제한 수의 자연인이 접근 가능하게 되는 것에 대해서 동의를 하거나, 해당 정보주체가 접근 가능하도록 한 것으로 볼 수 있는 조치를 한 경우를 의미한다. 이런 개인의 개입 없이는 접근 가능하게 되지 못하도록 해야 한다는 것이다[302].

3) 인증 메커니즘 활용

여기에서도 마찬가지로 GDPR은 인증메커니즘을 활용할 수 있다는 점을 규정하고 있다. 개인정보 감독기관에 의하여 승인된 인증 메커니즘은 기본설정에 의한 개인정보 보호의 준수 여부를 판단하는 수단이 될 수 있다.

---

301) 제25조 제2항
302) 제25조 제2항

3. 우리나라 개인정보 보호법의 규정과 개선방안

가. 설계 및 기본설정에 의한 개인정보 보호 도입 필요성

우리나라의 개인정보 보호법에는 설계에 의한 개인정보 보호나 기본설정에 의한 개인정보 보호에 관한 규정이 없다. 그 뿐만 아니라 개인정보처리자의 안전조치 의무도 협소하게 규정하고 있고, 보안과 관련한 안전조치 의무도 다소 형식적으로 규정되어 있기 때문에 우리나라의 개인정보 보호법은 개인정보 보호를 위한 수단이 통합된 개인정보 처리가 이루어지도록 하는 사전 규율이 미비하고, 신기술에 조응하는 개인정보 보호에도 취약하다. 이런 점을 고려한다면 설계 및 기본설정에 의한 개인정보 보호는 개인정보처리자의 책임 조항과 결합하여 매우 효과적인 사전예방의 수단이 될 수 있을 것이다.

나. 도입 방안

우리나라에서도 설계 및 기본설정에 의한 개인정보 보호 규정을 도입한다면, GDPR의 규정에 준하는 내용으로 도입할 수 있을 것이다. 개인정보 보호 설계를 할 때 고려할 사항으로 최신 기술, 실행 비용, 처리의 성격, 범위, 맥락 및 목적, 그리고 처리가 자연인의 권리와 자유에 대해 갖는 가능성과 심각성의 정도가 다양한 위험을 고려하도록 하는 것이 바람직할 것이다. 설계에는 개인정보 보호 법제가 요구하는 모든 사항을 준수해야 하고, 정보주체의 권리를 보호할 수 있는 조치를 포함해야 한다. 해당 기술적, 조직적 조치는 정보 최소화 등 개인정보 보호 원칙을 효과적인 방식으로 구현하고 필요한 보호조치를 처리에 통합하도록 설계해야 하며, 가명화 같은 조치도 포함된다는 점을 명시할 필요가 있다. 설계를 통해서 처리에 통합된 조직적, 기술적 조치의 적절성을 판단하는 시점은 처리 수단 결정 시점과 실제 처리 시점이 되어야 한다는 점도 분명하게 규정할 필요가 있다. 아울러 이를 준수하는 하나의 방안으로 인증 메커니즘을 활용할 수 있다. 그리고 개인정보 감독기관은 인증 시에 해당 인증 메커니즘이 설계에 의한 개인정보 보호를 준수하는지를 포함시키도록 하고, 이를 검토하여 승인함을 통해서 구체화시킬 수 있을 것이다.

아울러 기본설정에 의한 정보보호 규정도 도입할 필요가 있다. 특히 인터넷과 관련해

서는 기본설정을 통해 개인정보가 개인의 개입 없이 무제한 수의 자연인이 접근 가능하게 되지 않도록 보장해야 한다는 규정을 둘 필요가 있다.

제5절 개인정보보호 영향평가

1. 개요

개인정보 영향평가는 우리나라 개인정보 보호법에 2011년부터 도입되어 공공부문에서 일정한 규모 이상의 개인정보파일 운용 시에 사전 영향평가를 하도록 시행되고 있으며[303], 개인정보 보호의 사전예방적 기능을 수행할 수 있을 것으로 기대되었다. 그러나 개인정보 영향평가의 평가항목과 평가방법이 매우 형식적으로 이루어져 있어서 통과의례적인 평가로 기능할 수 밖에 없는 한계를 보이고 있다.

반면, 유럽연합의 GDPR에서도 개인정보보호 영향평가를 도입했는데, 공공부문과 민간부문을 불문하고 높은 위험을 초래할 가능성이 큰 경우에 적용되며, 사전에 개인정보 처리로 인한 위험을 파악하고 이를 억제할 수단을 평가하도록 하였다. 특히, 신기술, 자동의사결정, 대규모 시스템, 프로파일링 등에서 매우 중요한 역할을 할 것으로 기대되고 있다. 특히, GDPR의 규정은 영향평가의 과정을 평가하고 평가의 근거를 기술하도록 하고 있으며, 독립 정보보호 책임자(DPO)의 관여, 감독기관의 사전자문 절차, 개인정보 처리의 라이프사이클에 맞춘 지속적인 위험의 재평가 등을 명시하고 있다. 한국의 개인정보 보호 법제에서도 민간 분야를 포함하여 개인정보 영향평가를 실질화할 필요가 있다.

303) 개인정보보호법 제정 시 공공기관에 대하여 적용하는 것으로 도입되어 2011년부터 시행되었다.

2. GDPR의 규정

가. 개인정보보호 영향평가의 대상 : 고위험을 불러올 가능성이 있는 경우

1) 고위험을 불러올 가능성이 있는 경우

GDPR은 개인정보보호 영향평가를 개인정보 처리의 성격과 범위, 상황, 목적을 참작하여, 특히 신기술을 사용하는 처리 유형이 개인의 권리와 자유에 중대한 위험을 초래할 것으로 예상되는 경우(likely to result in a high risk to the rights and freedoms of natural persons)에 사전 영향평가를 하여야 한다고 규정하면서, 그에 대한 예시로 세 가지 경우를 들고 있다[304].

첫째, 프로파일링 등의 자동화된 처리에 근거한, 개인에 관한 개인적 측면을 체계적이고 광범위하게 평가하는 것으로 해당 평가에 근거한 결정이 해당 개인에게 법적 효력을 미치거나 이와 유사하게 개인에게 중대한 영향을 미치는 경우이다.

둘째, 특정범주의 개인정보에 대한 대규모 처리나 범죄경력 및 범죄 행위에 관련된 개인정보에 대한 처리에 해당하는 경우이다.

셋째는 공개적으로 접근 가능한 지역에 대한 대규모의 체계적 모니터링이다.

이들은 예시에 해당하며, 예시에 포함되지 않더라도 개인의 권리와 자유에 중대한 위험을 초래할 것으로 예상되는 경우에는 영향평가를 해야 한다.

2) 영향평가가 필요한 경우에 대한 분석

영향평가는 특히 신기술이 도입되는 경우에 유용성이 큰데, 어떤 경우 영향평가가 필요한지를 명확하게 규율하는 것은 쉽지 않다. GDPR은 기준을 세분하여 제시하고 있는데, 예시적인 규정이다. GDPR의 제35조(1)과 동조 (3)(a) 내지 (c)와 동조 (4) 전문 71, 75, 91이 영향평가가 필요한 경우의 예시들인데, 제29조 작업반은 GDPR의 시행 전에 이를 좀 더 명확하게 하기 위한 가이드라인으로서 의견서를 발표하였다[305]. 이에 따르면 다음

304) 제35조 제3항

305) ARTICLE 29 DATA PROTECTION WORKING PARTY(2017b), Guidelines on Data Protection Impact Assessment and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. wp248rev.01. Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017.

과 같이 세분화하고 있다[306].

첫째, 평가 및 점수 부여(scoring)의 경우이다. 정보주체의 직장에서의 실적, 경제 사정, 건강, 개인의 선호나 관심, 신뢰성이나 행동, 위치, 동선에 대한 평가나 점수 부여 등이다. 예를 들어 신용평가, 자금세탁, 반테러, 고객 건강평가 유전자 검사, 웹정보 기반 행동 프로파일, 마케팅 프로파일링이 여기에 해당한다.

둘째, 법적 효력 혹은 이와 유사한 중대한 영향을 미칠 수 있는 자동 의사결정이다.

셋째, 체계적인[307] 모니터링이 이루어지는 경우이다. 여기서 체계적이라는 것은 시스템에 의해서 모니터링이 이루어지거나(occurring according to a system), 사전에 준비되거나 조직되어 있거나 방법화되어 있는 것(pre-arranged, organised or methodical), 정보 수집의 일반적 계획의 일부로 이루어지는 경우(taking place as part of a general plan for data collection), 전략의 일환으로 이루어지는 경우(carried out as part of a strategy)를 의미한다. 네트워크를 통한 정보 수집도 마찬가지이다. 일반인이 접근할 수 있는 영역에 대한 체계적 모니터링도 이에 해당하는데, 이 경우는 정보주체가 인식할 수 없거나 피할 수 없기 때문이라고 한다[308].

넷째, 민감정보를 처리하는 경우이다.

다섯째, 대규모 정보처리를 하는 경우인데, 이 경우 그 정보주체의 수나 관련되는 정보주체 중 처리되는 인구의 비율을 고려하여 판단하기도 하고, 처리되는 정보의 항목들의 양이나 정보 항목의 범주의 다양성도 고려한다. 기간도 고려하고 영구적인지도 고려한다. 처리 활동의 지역적 범위도 고려한다.

여섯째, 개인정보를 매칭하거나 개인정보 세트를 통합하는 경우이다. 이는 다른 목적으로 수집된 정보, 다른 처리자에 의해 수집된 정보가 매칭되거나 통합되는 것으로, 정보주체의 합리적인 기대를 초과하기 때문이다.

일곱째, 취약한 정보주체와 관련된 정보의 처리인 경우이다. 이는 쉽게 동의 혹은 반대하기 어려운 점이나 권리 행사가 어려운 점을 고려한 것이다. 예를 들어 아동, 피고용인, 정신적으로 아픈 사람, 노인, 환자 등이 이에 해당한다.

여덟째, 정보의 혁신적 사용 혹은 정보처리 시 기술적·관리적 해결책을 적용하는 경우

306) Ibid., pp9-11.
307) Ibid., p4.
308) Ibid., p9.

이다. 이는 새로운 기술을 활용하는 것이기 때문에 그로 인한 영향을 파악할 필요가 있기 때문이다.

아홉째, 유럽연합 역외로의 정보 이전이 있는 경우이다.

열째, 정보처리 자체가 "정보주체로 하여금 본인의 권리행사를 막거나 서비스 혹은 계약을 이용하지 못하게 할 경우"이다. 이는 서비스 거부에 해당하기 때문에 권리나 자유에 큰 영향을 미치는 경우이다.

<표5-2> 개인정보보호 영향평가가 필요한지 여부에 대한 예시

개인정보 처리 사례	가능한 관련 기준	영향평가 시행 필요 여부
환자의 유전정보 및 의료정보를 처리하는 병원	- 민감 정보 - 취약층의 정보주체와 관련한 정보 - 대량 처리	필요함
고속도로상의 운전행태를 모니터링하기 위한 카메라 사용. 컨트롤러는 차량을 구별해 내고 번호판을 자동 인식하기 위해 지능형 비디오 판독 시스템을 활용할 것으로 예상됨	- 체계적인 모니터링 - 기술적·관리적 해결방안의 혁신적인 활용 및 적용	
피고용인의 작업장, 인터넷 작업 모니터링 등 피고용인의 활동을 모니터링 하는 회사	- 체계적인 모니터링 - 취약층의 정보주체와 관련한 정보	
프로파일을 생성하기 위해 공개 소셜 미디어 데이터 수집	- 평가 또는 점수 부여 - 대규모로 처리된 데이터 - 매칭과 조합 - 민감 또는 극히 개인적 속성	
국가 규모 신용 평가 또는 사기 관련 데이터베이스를 구축하는 기관	- 평가 또는 점수 부여 - 자동결정 - 권리행사 방해 - 민감 또는 극히 개인적 속성	필요함
연구 목적 또는 임상 실험을 위한 취약 정보주체의 가명화된 민감 개인정보를 기록보존 목적으로 저장	- 민감정보 - 취약층의 정보주체와 관련한 정보 - 권리행사 방해	필요함
구독인에게 일별 기사 요약본을 송부하기 위해 메일링 리스트를 활용하는 온라인 잡지	- (없음)	반드시 필요하지는 않음
과거 구매행태를 기반으로 제한적인 프로파일링이 수반되는 구형 자동차 부품 광고를 게시하는 전자상거래 웹사이트	- 평가 또는 점수 부여 - 체계적이거나 광범위하지 않음	

이런 기준을 바탕으로 예시되는 몇 가지 사안에서 개인정보보호 영향평가가 필요한지 여부를 평가하면 <표5-2>와 같다.[309]

3) 각국의 개인정보 감독기관이 공고한 개인정보보호 영향평가가 필요한 영역

한편, GDPR은 개인정보 감독기관으로 하여금 개인정보보호 영향평가가 필요한 영역에 대한 리스트를 명시할 수 있도록 하고 있다. 예를 들어 영국 ICO가 공고한 리스트에서는 ① 혁신적인 기술, ② 서비스 거부, ③ 대규모 프로파일링, ④ 생체인식 정보, ⑤ 유전정보, ⑥ 데이터 매칭, ⑦ 보이지 않는 처리, ⑧ 추적, ⑨ 어린이나 취약자에 대한 프로파일링, 마케팅을 위한 프로파일링, 자동화된 결정을 위한 프로파일링, ⑩ 신체적 위험으로 구분하고 있다. 반면, 프랑스의 경우는 14가지의 유형으로 분류하여 리스트를 공고하였다.

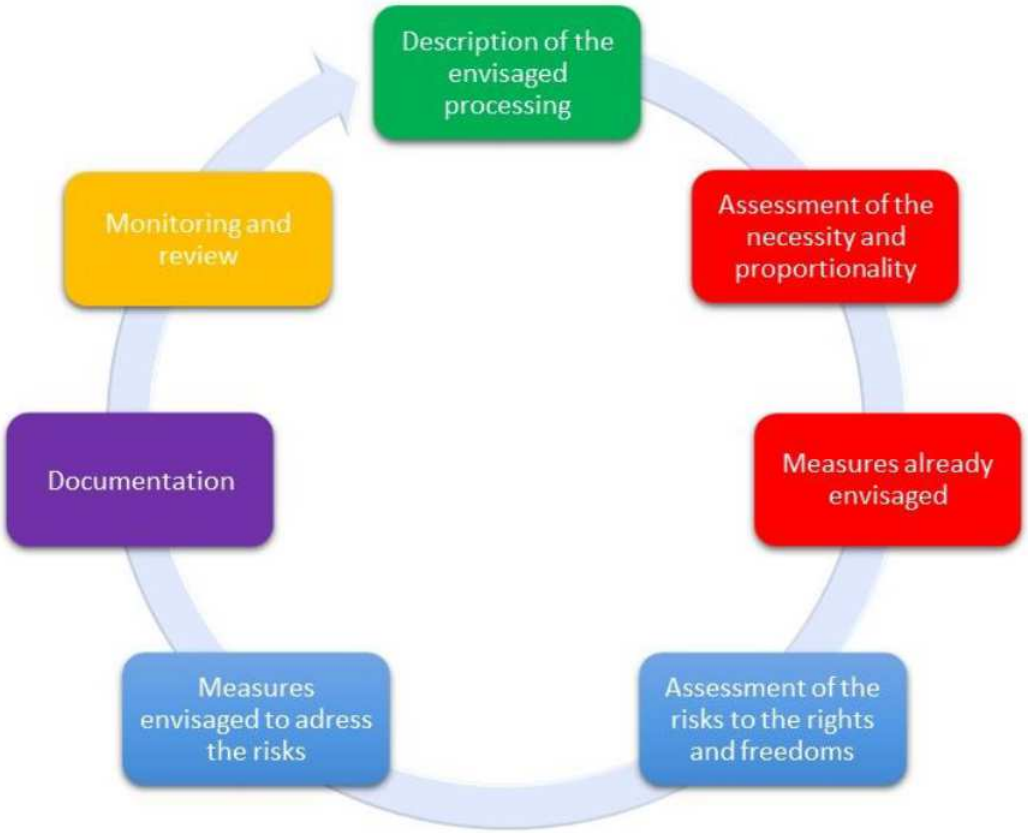
나. 개인정보보호 영향평가의 시기와 내용

1) 개인정보보호 영향평가의 시기

개인정보보호 영향평가는 컨트롤러가 처리 이전에 '예정된 처리 작업이 개인정보 보호에 미치는 영향에 대한 평가'를 시행하도록 하고 있다. 한편, 컨트롤러는 적어도 처리 작업으로 초래되는 위험에 변화가 있을 시에는 처리가 개인정보보호 영향평가에 따라 실시되는지를 평가하기 위한 검토를 시행해야 한다. 따라서 아래와 같은 라이프사이클의 구조를 갖추고 영향평가를 시행해야 한다. 단, 한 번의 평가로 유사한 중대한 위험을 초래하는 일련의 유사 처리 작업을 다룰 수 있다.[310]

309) Ibid., p11.
310) Ibid., p16.

<그림5-1> 개인정보보호 영향평가의 프로세스



2) 개인정보 영향평가의 내용

GDPR은 개인정보보호 영향평가가 포함해야 할 최소한의 내용을 규정하고 있다. 반드시 포함해야 할 사항은 다음과 같다[311].

첫째, 예상되는 처리 작업 및 컨트롤러의 정당한 이익 등 개인정보 처리의 목적에 대한 체계적인 설명이다. 이는 개인정보 처리를 하기 전에 먼저 예상되는 처리 작업의 처리 목적을 명확하게 밝히도록 함으로서 목적의 명확화에 기여를 할 것이다.

둘째, 목적과 관련한 처리 작업의 필요성 및 비례성에 대한 평가. 이처럼 먼저 목적을 명확하게 규정하고, 처리가 규정된 목적과 비교하여 필요성과 비례성을 충족하는지를 평가하도록 하는 것이다. 이는 최소수집의 원칙, 목적 명확화의 원칙을 평가하는 것이다.

311) 제35조 제7항

셋째, 제1항에 규정된 개인정보주체의 권리와 자유에 대한 위험성 평가. 이는 해당 개인정보의 처리로 인해서 개인정보주체의 권리와 자유에 어떤 위험이 초래될 수 있는 것인지, 그 영향은 무엇인지를 파악할 수 있게 하는 요소이다.

넷째, 개인정보주체와 기타 관련인의 권리 및 정당한 이익을 고려하여 개인정보의 보호를 보장하고 본 규정의 준수를 입증하기 위한 안전조치, 보안조치, 메커니즘 등 위험성 처리에 예상되는 조치. 이는 위험이 발생하는 경우 그 위험을 제어하는 수단으로 안전조치, 보안조치, 메커니즘이 적절한지를 평가하는 것이다.

한편, GDPR은 승인된 행동강령을 따르기로 하였다면, 영향평가를 할 때 이를 준수하는지를 고려해야 한다고 규정하고 있다. GDPR이 규정하는 개인정보보호 영향평가의 내용은 영향평가가 투명성을 보장하기 위한 것이라는 점을 잘 보여주고 있다.

3) 영향 평가과정에서 개인정보주체의 의견

GDPR은 적절한 경우, 컨트롤러는 상업적 이익이나 공익의 보호 또는 처리 작업의 보안을 침해하지 않고, 예정된 처리에 대한 개인정보주체 또는 그 대리인의 의견을 구해야 한다고 규정하고 있다.

다. 개인정보보호 영향평가 후, 감독기관의 사전 자문

1) 개인정보 감독기관의 사전 자문

한편, GDPR은 개인정보 감독기관의 사전 자문을 구하도록 하는 절차를 두어서 예정된 개인정보 처리가 초래하는 위험을 파악하고 그에 대한 위험 억제 수단을 적절하게 갖추지 못한 경우에는 개인정보 감독기관이 조치를 취할 수 있도록 하였다.

2) 개인정보 감독기관에 사전 자문을 얻어야 할 경우와 사전 자문 시 제공할 자료

GDPR은 개인정보보호 영향평가를 시행한 결과 처리가 고위험의 결과를 초래하는 경우로서, 컨트롤러가 그 위험을 완화하기 위해 취한 조치가 부재하는 경우에는 개인정보 처리 전에 개인정보 감독기관의 사전 자문을 구해야 한다는 규정을 두고 있다. 즉, 영향

평가에서 해당 개인정보 처리가 고위험을 초래할 가능성이 있는데, 컨트롤러가 그 위험을 상쇄시킬 수 있는 안전조치를 취할 수 없거나, 안전조치를 취하였지만 그 안전조치가 위험을 없앨 수 있는 적절한 수단으로 보기 어려운 경우에는 개인정보 처리 전에 개인정보 감독기관의 사전 자문을 얻도록 한 것이다.

컨트롤러는 이때 다음과 같은 자료를 감독기관에게 제공해야 한다. ① 가능한 경우, 처리에 관여하는 컨트롤러, 공동 컨트롤러 및 프로세서의 개별 책임, 특히 사업체집단 내의 처리에 대한 책임, ② 예정된 처리의 목적 및 방법, ③ 본 규정에 따라 개인정보주체의 권리와 자유를 보호하기 위해 제공되는 조치 및 안전조치, ④ 가능한 경우, 독립 정보보호 책임자(DPO)의 상세 연락처, ⑤ 개인정보보호 영향평가, ⑥ 감독기관이 요청한 기타 정보.

이때 감독기관이 해당 예정된 처리에 대해서 컨트롤러가 위험을 충분히 파악하지 못하였거나, 해당 위험을 완화하지 못한 경우 등 해당 처리가 개인정보 보호 규정을 위반할 것으로 의견을 제시하는 경우에는 8주 이내에 서면 형식의 권고를 제공해야 한다. 아울러 이때는 개인정보 처리를 하기 전이라도 처리의 정지 등의 조치를 취할 수 있다.

라. 고위험 개인정보 처리와 관련한 개인정보보호 영향평가의 흐름도

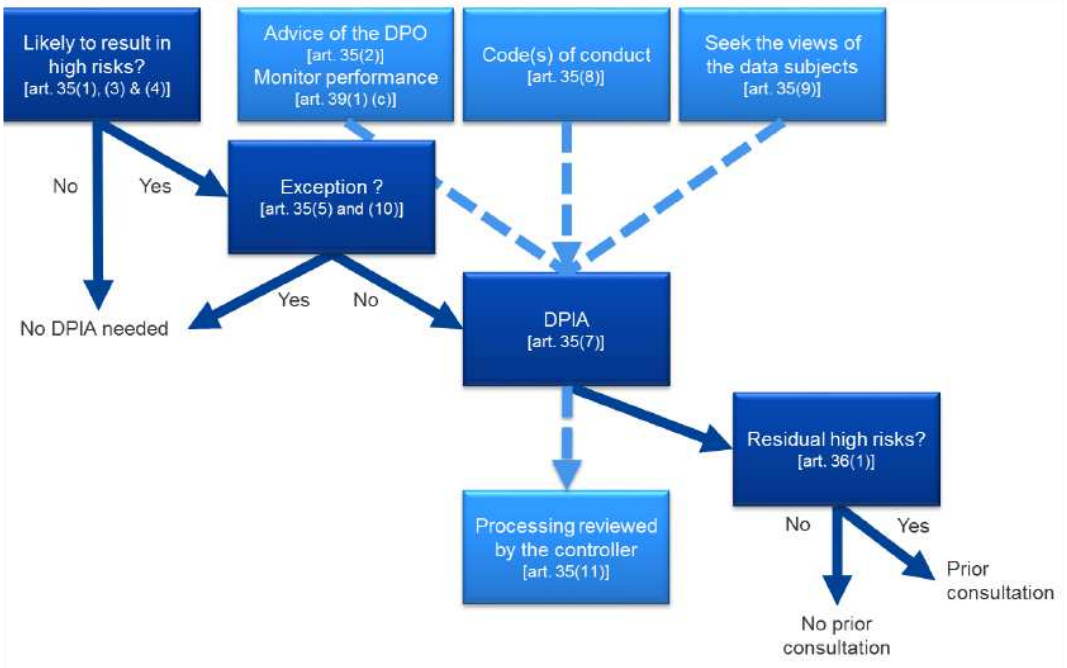
결국 GDPR에 의하면, 고위험의 개인정보 처리를 하는 경우에는 해당 개인정보 처리로 인해 발생할 수 있는 위험과 그에 대한 개인정보 컨트롤러의 조치가 적절한지를 평가하여야 하며, 그 결과 위험이 명확하게 파악되지 못하였거나, 위험을 없애기 위한 조치가 적절하고 충분하지 못하다면 개인정보보호 감독기관에 사전자문을 받도록 하여 그 위험을 사전에 검토, 평가하도록 한 것이다. 아울러 이 과정에서 관련 서류를 남기도록 함으로서 책임성과 투명성을 강화하는 것이다.[312]

마. 시사점

GDPR의 개인정보보호 영향평가와 사전협의는 고위험을 초래하는 개인정보 처리, 특히 신기술의 도입시에 매우 중요한 역할을 담당할 것이다. 영향평가 과정에서는 처리의 목

312) Article 29 Working Party(2017b), op. cit., p7.

<그림5-2> 개인정보보호 영향평가의 흐름도



적을 명확하게 하고, 그로 인해 발생할 수 있는 위험이 무엇인지를 명확하게 하고, 그에 대한 대응조치가 해당 위험을 억제할 수 있는 적절한 수준인지를 평가할 수 있게 하는 역할을 한다. 이는 매우 중요한 기능을 할 것이다.

3. 우리나라 개인정보 보호법의 개인정보 영향평가

가. 개인정보 영향평가의 대상

1) 공공기관의 경우

우리나라 개인정보 보호법은 개인정보 영향평가를 하는 대상을 공공기관으로 한정하고, 이를 개인정보파일에서 처리하는 개인정보의 종류와 양으로 규정하고 있다. 구체적으로, 공공기관에서 100만명 이상의 정보주체에 대한 개인정보파일을 구축, 운용, 변경하려는 경우나, 50만명 이상의 개인정보파일을 연계하려는 경우나, 5만명 이상의 민감정보나 고유식별정보 처리를 하는 경우에 영향평가가 필요하다고 규정하고 있다. 그래서 민

감정보나 고유식별정보를 처리하지 않는 경우라면 프로파일링이 이루어지거나, 지속적이고 체계적인 감시가 이루어지는 경우에도 개인정보 영향평가가 이루어지지 않을 수도 있게 된다. 기계적인 분류보다는 실질적인 개인정보 침해의 위험성에 기반하여 영향평가가 필요한 영역을 규정하는 것이 바람직하다.

2) 민간영역에서의 영향평가

개인정보 보호법은 공공기관 외의 개인정보처리자에 대해서도 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다(제33조 제8항)는 규정을 두고 있지만, 법률상 의무가 아닌 권유에 불과하여 사실상 실효성이 없다. 개인정보 영향평가는 특히 신기술과 관련해서 위험을 파악하고, 대응할 수 있는 효과적인 메커니즘인데, 그와 같은 신기술이 활용되는 주된 영역인 민간분야에 대해서 적용을 배제하고 있는 것은 문제이다. 개인정보 처리와 관련하여 고도의 위험이 발생할 수 있는 가능성이 있는 민간분야에 대해서도 개인정보 영향평가를 도입할 필요가 있다.

나. 영향평가 시 고려할 사항과 평가기준, 평가에 포함할 내용

개인정보 보호법은 개인정보 영향평가 시 고려할 사항을 규정하고 있는데, 이에는 처리하는 개인정보의 수, 개인정보의 제3자 제공 여부, 정보주체의 권리를 해할 가능성 및 그 위험 정도, 민감정보 또는 고유식별정보의 처리 여부, 개인정보 보유기간을 들고 있다(제33조 제2항). 그리고 평가기준으로는 다음의 4가지를 들고 있다(시행령 제38조 제1항).

(i) 해당 개인정보파일에 포함되는 개인정보의 종류·성질, 정보주체의 수 및 그에 따른 개인정보 침해의 가능성, (ii) 법 제24조제3항, 제25조제6항 및 제29조에 따른 안전성 확보 조치의 수준 및 이에 따른 개인정보 침해의 가능성, (iii) 개인정보 침해의 위험요인별 조치 여부, (iv) 그 밖에 법 및 이 영에 따라 필요한 조치 또는 의무 위반 요소에 관한 사항.

<그림5-3> 개인정보 영향평가에 관한 고시[별표 4]

[별표 4]

■ 개인정보 영향평가에 관한 고시 [별표 4]

개인정보 영향평가의 평가영역 및 평가분야 (제9조~제11조 관련)

(제1쪽)

평가 영역	평가 분야	세부 분야
Ⅰ. 대상기관 개인정보보호 관리체계	1. 개인정보 보호 조직	개인정보보호책임자의 지정
		개인정보보호책임자 역할수행
	2. 개인정보 보호 계획	내부관리계획 수립
		개인정보보호 연간계획 수립
	3. 개인정보 침해대응	침해사고 신고 방법 안내
		유출사고 대응
	4. 정보주체권리보장	정보주체 권리보장 절차 수립
		정보주체 권리보장 방법 안내
Ⅱ. 대상시스템의 개인정보보호 관리체계	5. 개인정보취급자 관리	개인정보취급자 지정
		개인정보취급자 관리·감독
	6. 개인정보파일 관리	개인정보파일대장 관리
		개인정보파일 등록
	7. 개인정보처리방침	개인정보처리방침의 공개
		개인정보처리방침의 작성
Ⅲ. 개인정보처리단계별 보호조치	8. 수집	개인정보 수집의 적합성
		동의 받는 방법의 적절성
	9. 보유	보유기간 산정
	10.이용·제공	개인정보 제공의 적합성
		목적 외 이용·제공 제한
		제공시 안전성 확보
	11. 위탁	위탁사실 공개
		위탁 계약
		수탁사 관리·감독
	12. 파기	파기 계획 수립
		분리보관 계획 수립
		파기대장 작성

(제2쪽)

IV. 대상시스템의 기술적 보호 조치	13. 접근권한 관리	계정 관리
		인증 관리
		권한 관리
	14. 접근통제	접근통제 조치
		인터넷 홈페이지 보호조치
		업무용 모바일기기 보호조치
	15. 개인정보의 암호화	저장시 암호화
		전송시 암호화
	16. 접속기록의 보관 및 점검	접속기록 보관
		접속기록 점검
		접속기록 보관 및 백업
	17. 악성프로그램 등 방지	백신 설치 및 운영
		보안업데이트 적용
	18. 물리적 접근방지	출입통제 절차 수립
		반출·입 통제 절차 수립
	19. 개인정보의 파기	안전한 파기
	20. 기타 기술적 보호조치	개발 환경 통제
		개인정보처리화면 보안
		출력시 보호조치
	21.개인정보처리구역보호	보호구역지정
V. 특정 IT기술 활용시 개인정보 보호	22. CCTV	CCTV 설치시 의견수렴
		CCTV 설치 안내
		CCTV 사용 제한
		CCTV 설치 및 관리에 대한 위탁
	23. RFID	RFID 이용자 안내
		RFID 태그부착 및 제거
	24. 바이오정보	원본정보 보관시 보호조치
	25. 위치정보	개인위치정보 수집 동의
		개인위치정보 제공시 안내사항

이와 같이 그 내용은 개인정보 침해가능성과 위험요인별 조치 여부이다. 한편 개인정보 보호위원회 고시인 '개인정보 영향평가에 관한 고시'는 평가항목을 구체화하고 있는데, 그 내용을 보면, 대상기관의 개인정보 보호 관리체계, 대상시스템의 개인정보 보호 관리체계, 개인정보처리 단계별 보호조치, 기술적 보호조치와 특정 IT 기술 활용 시의 보호조치이다.

그런데, 개인정보 보호법의 경우 영향평가에 포함시켜야 할 내용은 GDPR의 경우 해당 작업이나 목적에 대한 체계적인 설명에 이어서, 그 목적과 관련한 처리 작업의 필요성과 비례성 평가 등과 같이 먼저 체계적인 설명을 하고, 그에 대한 필요성과 비례성을 평가해야 한다는 내용이 분명하게 명시되어 있지 않다.

그리고 GDPR에서는 개인정보주체의 권리와 자유에 대한 위험성 평가, 개인정보주체와 기타 관련인의 권리 및 정당한 이익을 고려하여 개인정보의 보호를 보장하고 본 규정의 준수를 입증하기 위한 안전조치, 보안조치, 메커니즘 등 위험성 처리에 예상되는 조치를 명시하도록 하고 있는데 반해서, 개인정보 보호법은 이를 명시하고 있지 않다. 특히 GDPR은 영향평가의 목표가 처리에 따른 위험을 파악하는 것에도 두고 있는 것에 비추어 개인정보 보호법에서도 영향평가의 목표로 처리에 따른 위험을 구체화하여 식별해 내는 것에도 두고 이를 명시하도록 할 필요가 있다.

4) 영향 평가과정에서 개인정보주체의 의견

개인정보 보호법에서는 영향평가 과정에서 개인정보주체의 의견을 구해야 한다는 GDPR의 규정을 두고 있지 않다.

5) 영향평가에서 개인정보 보호위원회의 역할, 개인정보 보호책임자의 역할

개인정보 보호법은 공공기관이 영향평가를 하는 경우 그 결과를 보호위원회에 제출하여야 한다고 규정하고 있고(제33조 제1항), 개인정보파일을 등록할 때 영향평가 결과를 함께 첨부하도록 하고 있다(제4항). 그리고 보호위원회가 영향평가 결과에 대하여 의견을 제시할 수 있다고 규정하고 있다(제3항). 반면 민간분야의 경우는 개인정보 보호위원회는 아무런 역할도 규정되어 있지 않다. 독립 정보보호 책임자의 역할도 규정하고 있지 않다.

4. 개선방안

가. 민간분야 영향평가 제도 도입

우리 개인정보 보호법에도 민간분야에서도 개인정보 영향평가를 시행할 수 있도록 할 필요가 있다. 모든 민간분야에서 개인정보 영향평가를 수행하도록 하는 것보다는 고위험을 불러올 가능성이 있는 경우로 제한하여 운용할 수 있을 것이다.

고위험을 불러올 가능성이 있는 경우로는 GDPR에서 규정하는 예시를 참조할 수 있다. 즉, (i) 프로파일링 등의 자동화된 처리에 근거한, 개인에 관한 개인적 측면을 체계적이고 광범위하게 평가하는 것으로 해당 평가에 근거한 결정이 해당 개인에게 법적 효력을 미치거나 이와 유사하게 개인에게 중대한 영향을 미치는 경우나 (ii) 특정범주의 개인정보에 대한 대규모 처리나 범죄경력 및 범죄 행위에 관련된 개인정보에 대한 처리에 해당하는 경우, (iii) 공개적으로 접근 가능한 지역에 대한 대규모의 체계적 모니터링의 경우를 규정하는 것이 적절할 것이다.

나. 개인정보 보호위원회가 영향평가가 필요한 경우에 대한 기준 제시

어떤 경우에 영향평가가 필요할지를 명확한 문구로 규정하기는 쉽지 않다. 따라서 어떤 경우에 영향평가가 필요할지를 변화하는 신기술이나 새로운 서비스와 관련하여 적절하게 공개하는 것은 많은 도움이 될 것이다. 그래서 우리 법제에도 개인정보 보호위원회에 영향평가가 필요한 경우에 대한 지침을 제정할 수 있는 권한을 부여할 필요가 있다. 이에 따라 개인정보 보호위원회는 개인정보 처리의 성격상 개인정보 영향평가가 필요한 영역을 고시할 수 있을 것이다. 그에 해당하는 것으로 유럽연합에서 제시한 10가지의 기준이나, 영국 ICO의 기준, 프랑스 CNIL의 기준 등도 참고할 가치가 있다.

다. 개인정보 영향평가의 시기와 내용

개인정보 영향평가는 개인정보처리자가 개인정보를 처리하기 이전에 하는 것이 정상이다. 그러나, 개인정보의 처리 작업으로 초래되는 위험에 변화가 있을 때에도 영향평가

가 필요할 수도 있으므로 이에 대한 규율을 할 필요도 있다.

라. 개인정보 영향평가의 평가기준 및 내용

개인정보 보호법에서도 GDPR과 마찬가지로 개인정보 영향평가가 포함해야 할 최소한의 내용을 규정할 필요가 있다. 여기에는 (i) 예상되는 처리 작업 및 개인정보처리자의 정당한 이익 등 개인정보 처리의 목적에 대한 체계적인 설명, (ii) 목적과 관련한 처리 작업의 필요성 및 비례성에 대한 평가는 물론이지만 그와 함께, (iii) 개인정보주체의 권리와 자유에 대한 위험성 평가, 개인정보주체와 기타 관련인의 권리 및 정당한 이익을 고려하여 개인정보의 보호를 보장하고 본 규정의 준수를 입증하기 위한 안전조치, 보안조치, 메커니즘 등 위험성 처리에 예상되는 조치도 포함되어야 한다.

마. 영향평가 과정에서 개인정보주체의 의견 등

GDPR에서와 같이, 개인정보처리자로 하여금 상업적 이익이나 공익의 보호 또는 처리작업의 보안을 침해하지 않고, 예정된 처리에 대한 개인정보주체 또는 그 대리인의 의견을 구해야 한다는 규정을 도입할 필요가 있다.

바. 개인정보보호 영향평가 후의 개인정보 보호위원회의 사전 자문

GDPR은 개인정보 영향평가에도 불구하고 위험을 억제하는 적절한 수단을 갖추지 못한 경우에는 개인정보 감독기관에게 사전 자문을 구하게 하는 절차를 두고 있는데, 개인정보 보호법에도 해당 규정을 도입할 필요가 있다. 예정된 개인정보 처리가 초래하는 위험을 파악하고, 그에 대한 위험 억제 수단을 적절하게 갖추지 못한 경우에는 개인정보 보호위원회가 조치를 취할 수 있도록 할 수 있다. 이 규정을 도입하게 되면 고위험이 예상되는 개인정보 처리는 해당 처리가 도입되기 전에 개인정보 영향평가를 거쳐야 하고, 위험이 존재한다면 개인정보 보호위원회와의 사전협의를 거쳐야 하므로, 위험을 파악하고 통제할 수 있는 것으로 평가된 서비스만이 제공될 수 있게 하는 역할을 한다.

특히, 사전 자문 시에 ① 가능한 경우, 처리에 관여하는 컨트롤러, 공동 컨트롤러 및

프로세서의 개별 책임, 특히 사업체집단 내의 처리에 대한 책임, ② 예정된 처리의 목적 및 방법, ③ 본 규정에 따라 개인정보주체의 권리와 자유를 보호하기 위해 제공되는 조치 및 안전조치, ④ 가능한 경우, 독립 정보보호 책임자의 상세 연락처, ⑤ 개인정보 영향평가, ⑥ 감독기관이 요청한 기타 정보를 제공하도록 하는 규정을 도입하는 것이 바람직하다.

제6절 개인정보처리자의 처리 활동 기록 의무

1. 개요

개인정보 처리의 과정에서 개인정보처리자의 책임성을 보장하는 것은 매우 중요하다. 이와 관련하여 GDPR은 개인정보 처리의 원칙으로 '법률 준수에 대한 설명 및 증명의무'를 내용으로 하는 '책무성(accountability)' 원칙을 규정하고 있으며(제5조 제2항)[313], 이를 제24조에서도 컨트롤러의 의무로 규정하고 있는데, 그 일환으로 도입한 것이 '처리 활동 기록(Records of processing activities)'에 대한 의무이다. 즉, 컨트롤러와 프로세서로 하여금 개인정보 처리 활동기록을 보존하도록 의무를 부과한 것이다[314].

이 규정은 정보시스템이 매우 복잡하고, 개인정보의 처리가 정보주체가 접근할 수 없는 영역에서 이루어질 뿐만 아니라, 특히 디지털 데이터의 처리는 물리적으로 벌어지는 현상도 아니기 때문에 이를 확인하기도 어렵다는 점에서 필요성과 효용성이 있다. 예를 들어 컨트롤러나 프로세서의 행위로 인해 개인정보 침해가 이루어진 경우, 정보주체가 그에 대하여 컨트롤러나 프로세서를 대상으로 개인정보 보호법 위반으로 책임을 추궁하거나 그들의 과실을 입증한다는 것은 현실 환경에서는 거의 불가능에 가깝다. 이런 점을 고려하여 도입된 것이 처리 활동 기록(Records of processing activities)에 대한 의무이다. 컨트롤러에게 부여되는 처리 활동 기록 의무는 컨트롤러의 설명 및 입증의무(accountability)의 한 요소이다. GDPR도 전문에서 컨트롤러와 프로세서는 GDPR의 준수를 설명, 입증하기 위하여(In order to demonstrate compliance with this Regulation) 처리

313) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').
314) 제30조, 전문 13, 전문 82

활동 기록 의무를 부담하는 것이라고 명시하고 있다[315].

그런데 현재 우리나라 개인정보 보호법에서는 이와 같은 처리 활동 기록 의무가 없다. 대신 개인정보 처리방침에 중요한 사항을 기록하여 인터넷을 통해 공개하도록 하는 의무를 부과하고 있을 뿐이다. 그런데, 정태적인 개인정보 처리방침 게시 의무보다는 좀 더 적극적으로 동태적인 개인정보 처리 활동 기록 의무를 도입하여 개인정보 처리에서의 개인정보처리자의 책무성을 다하도록 하는 것이 바람직할 것이다.

2. GDPR의 규정

가. 처리 활동 기록 의무의 내용

GDPR은 개인정보 처리 활동과 관련한 기록을 하도록 하는 규정을 두고 있는데, 컨트롤러뿐만 아니라 프로세서에게도 기록 의무가 부과된다. 개인정보 처리와 관련해서 기록하고 보존하면서 독립 정보보호 책임자(DPO), 감독기관 등의 열람에 응하는 의무를 부담하게 된다. 한편 프로세서는 컨트롤러보다 기록 의무의 범위가 좁다.

컨트롤러가 부담하는 기록 의무는 다음과 같다. 첫째, 컨트롤러와 관련한 정보이다. 여기에는 컨트롤러나 공동 컨트롤러, 컨트롤러의 대리인, (해당하는 경우) 독립 정보보호 책임자의 이름과 연락처 세부사항이 포함된다.

둘째, 개인정보의 처리와 관련한 정보이다. 여기에는 다음과 같은 것들이 포함된다. (i) 정보 처리의 목적을 기록해야 한다. 정보 처리의 목적은 특정되고 명확해야 한다. (ii) 정보 주체의 범주와 개인정보의 범주에 관한 설명을 기록해야 한다. 처리하는 모든 개인정보를 개별적으로 열거하는 것은 불가능할 수 있으므로 개인정보의 범주와 정보주체의 범주로 기술하는 것이다. (iii) 개인정보를 제공받았거나 제공받을 예정인 수령자의 범주를 기술한다. 여기에는 제3국이나 국제기구의 수령자를 포함한다. (iv) 제3국이나 국제기구로 개인정보를 이전하는 경우에는 그에 대한 사실(해당 제3국 또는 국제기구의 정체 포함), GDPR 제49조제1항 2문에 의한 이전의 경우, 적합한 보호조치에 관한 문서, (v) 가능한 경우, 각기 다른 범주의 정보 삭제에 대한 예상 시한 등이다.

---

315) 전문 82

셋째, 기술적, 조직적 보안조치에 관한 일반적 설명도 가능한 범위에서 기록하도록 하고 있다. 기술적, 조직적 보안조치에 관한 일반적 설명을 서면으로 기록하도록 한 것은 큰 의미가 있다.

반면, 프로세서는 컨트롤러를 대신하여 수행한 모든 범주의 처리 활동에 관한 기록을 보존해야 한다. 여기에는 프로세서, 프로세서가 대행하는 컨트롤러, 컨트롤러 또는 프로세서의 대리인, 독립 정보보호 책임자의 이름과 연락처 세부사항, 각 컨트롤러를 대신하여 수행한 처리의 범주, 해당하는 경우 제3국이나 국제기구로의 개인정보 이전 사실(해당 제3국 또는 국제기구의 정체 포함), 또한 제49조제1항 두 번째 문단에 언급된 이전의 경우 적합한 보호조치에 관한 문서, 가능한 경우 제32조제1항에 언급된 기술적, 조직적 보안조치에 관한 일반적 설명을 기록해야 한다.

나. 적용의 면제

GDPR은 처리 활동 기록 의무를 종업원 250인 미만의 기업이나 단체에 대하여는 면제를 하고 있다. 단, 250인 미만인 경우에도 수행하는 처리가 정보 주체의 권리와 자유에 위험을 초래할 가능성이 큰 경우, 처리가 가끔씩만 이루어지는 것이 아닌 경우, 특수 범주 정보나 형사 판결 및 범죄 행위와 관련한 개인정보가 처리에 포함되는 경우는 면제되지 않는다.

다. 처리 활동 기록의 방법과 이용

처리 활동 기록은 전자문서나 서면으로 하도록 규정하고 있다. 해당 기록은 감독기관이 요청하는 경우 이용할 수 있도록 해야 한다. 이 기록은 컨트롤러나 프로세서가 GDPR을 준수하는지를 증명하는 수단이 될 것이다. 감독기관은 이 기록을 통하여 개인정보 처리를 모니터링 할 수 있게 된다[316].

316) 전문 82

3. 우리나라 개인정보 보호법의 처리 기록 의무

가. 개인정보 처리방침 명시의무

우리나라 개인정보 보호법에서는 개인정보처리자에게 개인정보 처리 활동 기록 의무를 규정하고 있지 않다. 반면, 개인정보 처리방침의 수립 및 공개의무(개인정보 보호법 제30조, 시행령 제31조)를 두고 있다. 여기에는 GDPR의 처리 기록 의무에 규정되어 기록해야 할 사항이 일부 포함되어 있다. 우리나라 개인정보 보호법에서 개인정보 처리방침에 구체적으로 적시해서 공개해야 하는 내용은 다음과 같다.

처리하는 개인정보의 항목, 개인정보의 처리 목적, 개인정보의 처리 및 보유 기간, 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다), 개인정보의 파기절차 및 파기방법(제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다), 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다), 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항, 개인정보 보호책임자의 성명 또는 개인정보 보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처, 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다), 제30조 또는 제48조의2에 따른 개인정보의 안전성 확보 조치에 관한 사항 등이다.

나. 홈페이지를 통한 일반 공개 의무

개인정보 처리방침은 이를 수립하거나 변경할 경우 개인정보처리자의 인터넷 홈페이지에 지속적으로 게재하도록 하고 있기 때문에 원칙적으로 '일반 공개'에 해당한다. 그런데, 공개해야 할 내용 중에는 개인정보처리자가 인터넷으로 일반 공개를 하는 것이 부담스러운 내용도 있는데, '개인정보의 안전성 확보조치에 관한 사항'의 경우, 인터넷에 공개할 경우 오히려 보안을 취약하게 할 수도 있다. 반면, GDPR은 이 내용을 서면으로 기록하도록 하면서도 일반 공개의무를 부과하지 않고, 감독기관에서 열람할 수 있도록만 하고 있다.

4. 개선방안

가. 처리 활동 기록 의무와 공개의 범위

우리 개인정보 보호법은 GDPR과 달리 개인정보 처리방침에 기재하는 내용은 인터넷의 홈페이지를 통해서 일반 공개를 하도록 하고 있다. 반면 GDPR은 일반 공개가 아닌 요청 시 제공할 의무로 규정하고 있다. 따라서 처리 활동 기록 의무를 범위를 나누어서 일반에게 공개할 사안과 일반에게 공개되는 것이 불합리한 사안에 대해서는 요구에 따른 제공 의무로 두는 것이 바람직해 보인다.

나. 무엇을 일반 공개로, 무엇을 요청 시 제공으로 할 것인가

예를 들어 개인정보 보호를 위한 안전조치의 내용은 일반 공개로 하는 경우, 오히려 보안을 취약하게 할 수도 있기 때문에 일반 공개보다는 요청 시 제공으로 하는 것이 적정할 수 있다. 개인정보 수집의 목적 등은 널리 일반 공개를 하더라도 문제가 없을 수 있다. 따라서 처리의 내용을 기록하도록 하되, 일반 공개의 대상과 요구 시 제공의 대상으로 나누는 것이 좋을 것이다.

제7절 개인정보 침해 통지 제도

1. 개요

우리나라 개인정보 보호법에는 개인정보 침해 통지 제도가 규정되어 있는데, 유럽연합의 경우 과거 디렉티브(95/46/EC)에는 없던 개인정보 침해 통지에 관한 규정을 GDPR에서 새로 도입하였다[317]. GDPR의 경우는 침해 통지의 요건에서 개인정보 침해가 자연인의 권리와 자유에 대한 위험을 초래할 가능성이 낮은 경우는 예외로 두고 있는데, 우리나라 개인정보 보호법에서는 그와 같은 예외 규정을 두고 있지 않다. 따라서 개인정보 침해가 발생하는 모든 경우에 침해 통지를 하여야 한다.

317) GDPR 제33조

2. GDPR 규정

가. 개인정보 침해 통지 제도의 도입

GDPR은 감독기관에 대한 개인정보 침해 통지와 정보주체에 대한 침해 통지로 두 가지를 규정하고 있다. 침해 통지를 할 요건은 개인정보 침해가 자연인의 권리와 자유에 대한 위험을 초래할 가능성이 낮지 않은 경우이다. GDPR은 '개인정보 침해'를 '전송, 보관,, 처리되는 개인정보가 우발적이거나 불법적으로 파괴, 손실, 변경, 무단 공개나 그에 대한 접근으로 이어지는 보안 침해를 의미한다'고 규정하고 있다.

통지해야 할 내용에는 가능하다면 관련 개인정보주체의 범주 및 대략적인 수, 관련 개인정보 기록의 범주 및 대략적인 수 등을 포함한 개인정보 침해의 성격에 대한 설명, 독립 정보보호 책임자 또는 추가 정보를 얻을 수 있는 기타 연락 창구의 이름과 연락처 세부사항, 개인정보 침해의 예상 결과에 관한 설명, 적절한 경우 가능한 악영향을 완화하기 위한 조치를 포함하여 개인정보 침해를 해결하기 위해 컨트롤러가 취했거나 취할 예정인 조치에 관한 설명 등이다. 아울러 개인정보 침해와 관련한 사항은 문서화를 해야 한다.

한편, 정보 주체에 대한 개인정보 침해 통지는 개인정보 침해가 자연인의 권리와 자유에 높은 위험을 초래할 가능성이 큰 경우에 해야 한다. 이 경우 컨트롤러는 지체 없이 정보주체에게 개인정보 침해 사실을 알려야 한다. 이때는 명확하고 평이한 표현을 사용하여야 한다. 알릴 내용은 개인정보 침해의 성격을 설명하고, 최소한 '독립 정보보호 책임자 또는 추가 정보를 얻을 수 있는 기타 연락 창구의 이름과 연락처 세부사항', '개인정보 침해의 예상 결과에 관한 설명', '개인정보 침해를 해결하기 위해 정보 컨트롤러가 취했거나 취할 예정인 조치에 관한 설명(적절한 경우, 가능한 악영향을 완화하기 위한 조치 포함)이다. 컨트롤러가 정보 주체에게 개인정보 침해 사실을 아직 알리지 않은 경우, 해당 개인정보 침해가 높은 위험을 초래할 가능성이 크다고 생각한 감독기관은 컨트롤러에게 통지를 요구하거나 아래에 언급된 조건 중 어느 하나를 충족시키도록 결정할 수 있다.

나. 정보주체에의 침해 통지를 하지 않아도 되는 경우

컨트롤러가 적절한 기술적, 조직적 보호 조치를 이행했으며, 그러한 조치, 특히 암호화 등 정보에 대한 접근이 허가되지 않은 사람은 개인정보를 이해할 수 없게 하는 조치가 개인정보 침해에 영향을 받은 개인정보에 적용된 경우, 컨트롤러가 정보 주체의 권리와 자유에 대한 중대한 위험이 실현될 가능성이 더 이상 크지 않도록 하는 후속 조치를 취한 경우, 해당 통지가 과도한 노력을 요구하는 경우(단, 해당 경우는 일반 대중을 대상으로 한 통지 또는 동일하게 효과적인 방식으로 정보 주체에게 사실을 알릴 수 있는 유사한 조치가 대신 이루어져야 한다)에는 정보주체에게 통지하지 않아도 된다.

3. 우리나라 개인정보 보호법 규정

가. 규정

우리나라 개인정보 보호법은 개인정보 유출통지에 대한 규정을 두고 있는데, 대체로 GDPR의 규정과 대동소이하다.

나. 양자의 차이

양자의 가장 큰 차이는 GDPR은 모든 개인정보 침해를 통지의 대상으로 하지 않고, 위험 발생의 우려를 기준으로 하고 있는데 반하여 우리 개인정보 보호법은 침해 통지를 하지 않아도 되는 경우를 규정하지 않고 있다.

제8절 독립 정보보호 책임자(Data Protection Officer)

1. 개요

2001년에 유럽연합의 기구나 조직의 개인정보 처리에 대해서 규율하는 유럽연합 규정인 Regulation 45/2001[318]이 제정되었는데 이 규정에서 처음으로 독립성을 가지면서 개인

318) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18

정보 보호 감독 업무를 수행하는 독립 정보보호 책임자(Data Protection Officer, DPO)[319] 제도가 도입되었다.[320][321] 유럽 개인정보보호감독관(European Data Protection Supervisor, EDPS)[322]은 DPO 제도에 대하여 매우 유용한 시스템으로 기능해 왔다고 평가하면서[323], 향후에도 EDPS와 상호 협력하면서 개인정보 보호 법률의 준수를 효과적으로 담보할 수 있는 기구로 보완, 발전시켜 나갈 것을 제안하는 입장문(position paper)을 두 차례에 걸쳐서 발표했다(2005, 2018)[324]. 실제로 유럽연합 기구들의 DPO들은 DPO Network(Network of Data Protection Officers of the EU institutions and bodies)를 구성하여 활발한 활동을 하고 있으며[325], 2010년에는 유럽연합 규정 45/2001에 의한 유럽연합 기구와 조직의 DPO의 전문성 기준이라는 보고서를 발표하기도 하였다. 이 보고서에 행위 모범 기준(best practice)과 DPO 윤리기준(ethical standards for dpos)이 포함되어 있다[326].

December 2000, on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

319) 우리나라 개인정보 보호법에는 개인정보 보호책임자라는 제도가 도입되어 있다. 그런데. 이는 GDPR의 Data Protection Officer라는 제도와는 아주 큰 차이가 있다. 특히 가장 큰 차이는 '독립성'에 있는데, 현재 우리나라 개인정보 보호법에 도입되어 있는 개인정보 보호책임자는 독립성을 보장받지 못하고 있다. 그래서 이 글에서는 Data Protection Officer를 '독립 정보보호 책임자'로 번역하였다.

320) Regulation 45/2001 제24조

321) 현재는 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.)으로 변경되어 시행 중이다.

322) 유럽연합 기구나 조직의 개인정보 처리에 대한 감독권한을 갖는 기구.

323) 유럽연합의 EDPS는 DPO가 매우 중요한 역할을 담당하고 있다고 판단하여 유럽연합 조직이나 기구에 설문지를 배포하여 DPO와 관련한 규정의 준수 여부를 모니터링하고, 그 결과를 보고서로 발표하였다. Monitoring compliance of EU institutions and bodies with Article 24 of Regulation (EC) 45/2001 Report on the Status of Data Protection Officers.

324) EDPS(2005), Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, 2005. 11. 28. EDPS(2018), Position paper on the role of Data Protection Officers of the EU institutions and bodies, 2018. 9. 30.

325) 현재의 DPO 명단을 공개하고 있다. <https://edps.europa.eu/node/53>.

326) Network of Data Protection Officers of the EU institutions and bodies(2010), Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001, 2010. 10. 14. pp13-15.

GDPR은 이와 같이 효용성이 검증된 DPO를 유럽연합 기구와 조직이 아닌 유럽연합 내의 공공기관과 민간 분야에 대해서까지 도입하게 된 것이다[327]. 실제로 GDPR 제정 과정에서 각국의 개인정보 감독기관의 협의체인 제29조 작업반은 DPO는 책임 보증의 원칙(accountability)의 주춧돌이라고 주장하고, 이는 기업의 경쟁력 확보의 원천이 될 수 있다면서 반드시 도입되어야 한다는 의견을 피력하기도 했다[328]. 이처럼 GDPR은 DPO 제도를 개인정보 보호를 위한 체계의 핵심적 내용으로 보고 있다. 그래서 GDPR은 DPO에게 개인정보 보호법의 준수를 보장, 감독할 수 있는 지위와 역할을 충분히 보장하고, 그 동안 DPO Network와 EDPS에 의하여 DPO 제도 성공의 핵심 요체로 제기되어 온 '독립성'과 '전문성'을 보장하기 위한 내용을 규율에 포함하고 있다[329]. GDPR이 2018년 5월부터 시행되면서, 유럽연합 각국에서는 DPO의 자격에 대한 규율이 만들어지고 DPO가 임명되고 있으며, 그들의 조직도 만들어지고 있다. 이들은 향후 개인정보 보호에 관하여 전문성과 독립성을 가지고 추진하는 독특한 지위의 역할을 해 나갈 것으로 기대된다.

반면, 우리나라는 개인정보 보호책임자를 두도록 하는 규정을 두고 있는데, 이들은 독립성을 지닌 자가 아니라 개인정보 업무를 총괄 책임지는 역할을 하는 자로서 규정되고 있고, 그에 따른 역할을 하고 있다. 이들에게서는 독립성을 가진 기능을 기대할 수 없다. 우리나라 개인정보 보호법에서도 독립성과 전문성을 가진 DPO 제도를 도입할 필요가 있으며, 아울러 공공기관의 경우에는 이들의 네트워크 등도 활성화될 수 있도록 보장하는 것이 바람직할 것이다.

2. 독립 정보보호 책임자(DPO)에 대한 GDPR 규정

GDPR은 새롭게 유럽공동체의 기구나 조직 외의 영역에서도 DPO를 임명하도록 제도를 도입했는데, 그 내용은 다음과 같다.

---

327) ARTICLE 29 DATA PROTECTION WORKING PARTY(2017c), Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01. Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017.

328) Ibid.

329) GDPR 제37조 ~ 제39조

가. 누가 DPO를 지정해야 하는가?

GDPR에서는 모든 컨트롤러가 DPO를 지정해야 할 의무가 있는 것이 아니라 일정한 요건을 갖춘 경우에만 지정하도록 하고 있다[330]. GDPR이 DPO를 지정할 의무를 부과한 경우는 (i) 공공기관이나 공적 업무를 수행하는 조직인 경우와 (ii) 개인정보 처리와 관련하여 위험성이 높은 경우이다. 그 외에 임의적으로 지정하는 경우가 있을 수 있는데, 이 경우도 DPO의 권한과 임무 등과 관련된 규정이 적용된다.

그 중 첫 번째로는 공공기관이나 공공단체의 경우이다.[331] 처리업무의 종류나 유형, 규모와 관계없이 모든 공공기관이나 공공단체는 DPO를 두도록 하고 있다. 다만, 그 수는 정보처리의 내용이나 조직의 크기 등을 고려하여 정할 수 있도록 하여, 여러 조직을 통할하여 업무를 수행할 수 있도록 하고 있다. 따라서 모든 공공기관과 공공단체에는 개인정보 보호와 관련하여 법률 준수 여부를 감독하고, 전문적인 자격을 갖추고 조언을 할 수 있는 독립성을 가지고 직무를 담당하는 책임자가 임명되어야 하는 것이다. GDPR은 공공기관이 직접 공적인 업무를 수행하는 경우뿐만 아니라, 공공의 업무를 민간 기관이나 개인에게 위탁하는 경우도 이에 해당하는 것으로 보고 있다. 예를 들어 공공교통 역무, 수도나 에너지 공급, 도로 인프라, 공공 방송, 공공 주택 공급 등의 공공 역무가 수행되는 과정에서 개인정보가 처리되는 경우이다[332]. 공공기관이나 공공단체가 DPO를 두도록 한 이유는 업무의 적법성을 꾀할 수 있도록 하기 위함이고, 공공기관이나 공공단체의 개인정보 처리는 개인정보주체가 이를 회피할 수도 없기 때문이기도 하다[333].

둘째는 컨트롤러나 프로세서의 핵심 활동(core activities)이 정보주체에 대한 대규모의 정기적, 체계적 모니터링을 필요로 하는 처리 작업으로 구성되는 경우이다[334]. 핵심 활동이란 부수적인 활동(ancillary activities)으로 개인정보를 처리하는 경우가 아니라 주된 활동(primary activities)으로 개인정보를 처리하는 경우를 말한다[335]. 컨트롤러나 프로세서의 목적을 달성하기 위하여 필요한 중요 업무로 볼 수 있는 것을 '핵심 활동'으로 볼 수

330) 제37조 제1항
331) 제37조 제1항 (a)
332) ARTICLE 29 DATA PROTECTION WORKING PARTY(2017c), op. cit., p6.
333) Ibid.
334) 제37조 제1항 (b)
335) ARTICLE 29 DATA PROTECTION WORKING PARTY(2017c), op. cit., p7.

있을 것이다. 이와 관련하여 제29조 작업반의 DPO 가이드라인(2016. 12. 13.)에서는 개인정보 처리가 해당 컨트롤러나 프로세서 활동에서 분리할 수 없는 일부를 구성하고 있는 경우는 핵심 활동이라고 한다. 이를 판단할 때 그 성격, 범위 및 목적을 고려한다. 아울러 대규모인지 여부를 판단하는 데 있어서는 개인정보 주체의 수, 개인정보의 양과 처리되는 데이터 항목의 범위, 처리 활동의 기간이나 영속성 여부, 처리 활동의 지리적 범위 등을 고려한다.

셋째는 컨트롤러나 프로세서의 핵심 활동이 특별 범주의 정보와 형사 판결 및 범죄행위와 관련된 개인정보의 대규모 처리로 구성되는 경우이다[336].

넷째는 각국의 법률이 추가적으로 개별 컨트롤러나 프로세서, 또는 해당 범주를 대표하는 협회나 그 밖의 단체에게 DPO를 지정하도록 규정하거나, 임의로 지정을 하는 경우이다[337]. 만약 임의로 지정하고 보고를 하는 경우에는 권한은 부여되어야 한다.

DPO가 선임되어야 하는 조건인지 여부에 대해서는 내부적인 분석을 하여 기록으로 남겨 놓아야 한다고 보고 있다[338].

나. DPO의 수

원칙적으로는 요건에 해당하는 컨트롤러나 프로세서는 각자 DPO를 선임해야 한다. 다만, 사업자 집단을 구성하는 자들이나, 공공기관이나 공동단체인 경우는 통합하여 DPO를 지정할 수 있다[339]. 이 경우, 사업자 집단의 경우는 각 사업장에서 DPO에게 쉽게 접근할 수 있어야 하고, 컨트롤러나 프로세서가 공공기관 또는 공공단체인 경우, 조직 구조와 규모를 고려하여 그러한 여러 기관 또는 단체에 대해 단일 DPO를 지정할 수 있다.

다. DPO의 자질과 자격

DPO는 전문가로서의 자질과 특히 정보보호 법률 및 관행에 관한 전문지식, 그리고 제39조에 언급된 업무를 완수할 수 있는 능력을 바탕으로 지정되어야 한다[340]. 이와 같은

336) 제37조 제1항 (c)
337) 제37조 제4항
338) ARTICLE 29 DATA PROTECTION WORKING PARTY(2017c), op. cit., p5.
339) 제37조 제2항, 제3항.

자질에 대한 규정은 DPO가 처음 도입되었던 Regulation 45/2001에서부터 유지되어 온 것이다[341]. 유럽연합의 DPO Network(Network of Data Protection Officers of the EU institutions and bodies)는 DPO의 직무기준(Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001)에서도 이 점을 강조하였다[342]. 여기서는 개인정보 보호에 대한 전문적인 지식과 전문가로서의 자격(Professional qualities and expert knowledge of data protection)으로 해당 법제에 대한 지식과 IT와 IT 보안에 대한 전문지식, 기관의 운영과 개인정보 처리 활동에 대한 이해 및 이를 적절한 개인정보 보호 규칙들에 맞추어 해석할 수 있는 좋은 이해력을 제시하고, 개인적 자격(Personal qualities which the DPO should possess)으로 해당 분야에서 7년(개인정보 처리가 핵심 활동인 분야의 경우) 또는 3년(개인정보 처리가 핵심 활동인 분야가 아닌 경우) 이상의 경험이 필요하고, 그 외의 개인적인 자질과 다른 사람과의 대인적 자질을 제시하고 있다. 그리고 임명 후의 훈련 및 자격의 취득기회에 대해서도 규정하고 있다.

각국은 법령에서 DPO에게 요구되는 능력과 자질에 대한 규정을 두기도 한다. 예를 들어 프랑스 개인정보 보호법은 개인정보 보호 감독기관인 CNIL(Commission Nationale de l'Informatique et des Liberts)로 하여금 DPO의 자격에 대하여 인증할 수 있는 인증기관을 승인할 수 있는 권한을 갖도록 규정하였고[343], 그에 따라 CNIL은 DPO의 기술과 지식의 인증을 위한 기준을 제시하고 있다[344][345]. 그러나 이는 지식과 기술(knowledge and skills)의 인증으로서 해당 자격증이 DPO로 임명되기 위한 요건은 아니며[346], 해당 자격

340) 제37조 제5항, 전문 97
341) 제24조 제2항
342) Network of Data Protection Officers of the EU institutions and bodies(2010), cp. cit., pp3-6.
343) Act no. 78-17 of 6 January 1978, amended, on information technology, data files and civil liberties, particularly Article 11-I-2 f bis).
344) CNIL(2018), Certification des comptences du DPO : la CNIL adopte deux rfrentiels 11 octobre.
345) Deliberation no. 2018-317 of 20 September 2018 adopting the criteria for the accreditation of certification bodies for the certification of data protection officer (DPO) skills and knowledge.
346) CNIL, 2018,11.1, "CERTIFICATION SCHEME OF DPO SKILLS ANDKNOWLEDGE", <https://www.cnil.fr/sites/default/files/atoms/files/cnil_certification-scheme-dpo-skills-and-knowledge.pdf>.

증은 자발적인 것으로 규정하고 있다. 한편, DPO의 지식과 기술의 인증은 CNIL이 인증한 기관에서 시험을 통해서 받는데, 인증기관으로는 LCP CERTIFICATION FRANCE, AFNOR CERTIFICATION, LSTI, PECB, IAPP (International Association of Privacy Professionals), SGS, CESI CERTIFICATION, APAVE CERTIFICATION 등이 승인되었다. 이들 인증기관들은 독립성을 가지고 있는 기관들이며, 주로 여러 유형의 자격증에 대한 시험과 인증을 담당하는 조직체이다.

라. DPO의 유형

DPO는 컨트롤러나 프로세서의 직원으로서 업무를 수행할 수도 있고, 외부인과의 서비스 계약을 기초로 업무를 수행할 수도 있다[347]. 컨트롤러나 프로세서는 DPO의 연락처 세부사항을 게시하고 이를 감독기관에 알려야 한다[348].

마. DPO의 지위

첫째, DPO는 개인정보 보호와 관련한 모든 문제에 관여하도록 보장되어야 한다. 아울러 적시에 적절한 방식으로 관여할 수 있도록 보장해야 한다[349]. 만약 이를 위반한다면, 이는 규정의 위반이 될 것이다. 이와 관련하여 가능한 가장 빠른 시점에 해당 문제에 관여할 수 있도록 보장되는 것이 매우 중요하다고 한다. 해당 문제에 대한 DPO의 조언이 이루어질 수 있도록 보장되어야 한다는 것이다. 이처럼 가능한 빠른 시점에 관여를 보장하는 것은 설계에 의한 개인정보 보호를 실제로 보장하고 촉진하는 수단이 될 것이다[350]. 제29조 작업반의 가이드라인은 이와 관련하여 다음과 같은 것들이 보장되어야 한다고 제시한다[351].

- DPO는 정기적으로 상급 경영관련 회의나 중간 경영관련 회의에 초대되어야 한다.

---

347) 제37조 제6항
348) 제37조 제7항
349) 제38조 제1항
350) ARTICLE 29 DATA PROTECTION WORKING PARTY(2017c), op. cit., p13.
351) Ibid., pp13-14.

- 개인정보 보호와 관련된 결정을 할 때 DPO가 참관할 수 있도록 권유된다.
- DPO가 충분한 조언을 할 수 있도록 적시에 DPO에게 적절한 정보가 제공되어야 한다.
- DPO의 의견은 항상 적정한 무게감으로 주어져야 한다. DPO의 의견을 따르지 않을 때, 제29조 작업반은 DPO의 의견을 따르지 않는 이유를 문서화 하는 것을 모범 행위의 사례로 권고한다.
- 개인정보 침해나 다른 사고가 발생했을 경우 즉시 DPO와 상의를 하여야 한다.

둘째, 필요한 자원 제공과 지원의무가 있다. 즉, 컨트롤러와 프로세서는 DPO가 자신의 업무를 수행할 수 있도록 해당 업무와 개인정보 및 처리 작업에 대한 접근을 수행하고 전문지식을 유지하는 데 필요한 자원을 제공하여 DPO를 지원해야 한다[352]. 필요한 자원이라면 관리적인 측면에서의 권한 부여, 물리적 차원의 수단 제공 등이 이루어져야 할 것이다. 최고위급으로부터의 DPO에 대한 적극적인 지원, 직무를 수행하기 위한 충분한 시간, 재정, 인력, 조직적 자원, 모든 직원들에게 DPO의 지정에 대하여 공지, 예를 들어 인사, 법무, 정보통신, 보안 등과 같은 관련자에 접근, 지속적인 훈련, 조직의 구조나 규모에 따라서는 DPO 팀의 구성 등도 제공되어야 한다[353].

셋째, 지시 금지이다. 컨트롤러와 프로세서는 DPO가 자신의 업무 수행과 관련하여 어떠한 지시도 받지 않도록 보장해야 한다[354]. 아울러 해당 조직에서 DPO가 독립적이고 자율적인 업무수행을 할 수 있는 보장이 이루어져야 한다. 예를 들어 어떤 결과가 나와야 하는지, 권리구제 청구를 어떻게 조사할지 또는 감독기관과 협의할지 여부 등과 같은 것에 대해서 지시를 받아서는 안 된다는 것이다. 또한, 법률의 해석이나 적용 등에 대해서도 지시를 받아서는 안 된다는 것이다.

그러나 DPO의 자율성은 제39조에서 부여된 DPO의 권한을 행사하는 것을 넘어서서 결정권을 갖는다는 것을 의미하지는 않는다. 만약 컨트롤러나 프로세서가 DPO의 의견과 다르게 결정을 내리는 경우 DPO는 해당 결정을 내리는 최고위의 책임자에게 자신의 의견을 명료하게 전달할 수 있는 기회가 제공되어야 한다. 이와 관련하여 GDPR 제38조 제

352) 제38조 제2항
353) ARTICLE 29 DATA PROTECTION WORKING PARTY(2017c), op. cit., p14.
354) 제38조 제3항

3항은 DPO가 최고위의 경영자에게 직접 보고를 할 수 있어야 한다고 규정하고 있다. 이와 같은 직접 보고에 의하여 최고위 경영자(예를 들어 이사회의 이사들)들이 DPO의 조언과 권고를 알게 되는 것이다. DPO의 직접 보고의 다른 예는 DPO가 최고위 경영진에게 제공하는 연례보고서이다[355].

넷째, 불이익 금지이다. DPO는 업무 수행을 이유로 컨트롤러와 프로세서에 의해 해고되거나 처벌을 받아서는 안 된다[356]. 그러나 업무 수행과 관련한 규정 위반으로 불이익을 받는 것은 허용된다고 한다.

다섯째, 직접 보고이다. DPO는 컨트롤러나 프로세서의 최고 경영진 수준에 직접 보고해야 한다[357]. 이를 통해서 최고 경영진은 개인정보와 관련된 업무에 대해서 DPO를 통하여 보고를 받게 되는 것이고, 이 보고를 바탕으로 책임을 준수할 의무가 따르게 될 것이다.

여섯째, 정보주체의 연락가능성이다. 정보주체가 자신에 관한 개인정보 처리와 본 규정에 따른 권리 행사와 관련한 모든 문제에 관해 DPO에게 연락할 수 있도록 보장을 해주어야 한다[358].

일곱째, 이해충돌의 금지이다. DPO는 다른 업무 및 임무를 수행할 수 있지만, 그런 업무 및 임무가 이해충돌을 초래하지 않도록 보장해야 한다[359]. 이해충돌의 금지를 요하는 이유는 독립성을 보장하기 위함이다. 이해충돌로 간주되는 직위로는 상급 경영자(예를 들어 CEO, COO, CFO, CMO, 마케팅 부문장, 인사부문장, IT 부문장 등)는 물론이고, 만약 해당 직위가 개인정보 처리의 목적과 수단을 결정하는 역할을 하게 된다면 이해충돌이 발생하게 된다. 뿐만 아니라, DPO가 개인정보 보호와 관련된 소송에서 해당 업무를 담당하는 경우에도 이해충돌이 있다고 본다[360]. 만약 DPO가 사업주이거나, 이사, 파트너, 대표이사나 경영주, 이사회 의장 등인 경우에는 당연히 이해충돌이 발생하고, 독립성이 보장되지 않을 것이다[361].

---

355) ARTICLE 29 DATA PROTECTION WORKING PARTY(2017c), op. cit., p15.
356) 제38조 제3항
357) 제38조 제3항
358) 제38조 제4항
359) 제38조 제6항
360) ARTICLE 29 DATA PROTECTION WORKING PARTY(2017c), op. cit., p16.
361) OneTrustDataGuidance, 2019.10., “Germany: The role of the DPO and conflicts of interest”,

DPO의 이해충돌 직무수행 금지 위반으로 벌금을 부과한 사안은 다음과 같다.

- 2020. 4. 28. 벨기에 개인정보 감독기관(Belgian Data Protection Authority)은 이해충돌이 있는 직무를 수행하고 있는 DPO를 선임한 기업에 대하여 50,000유로의 벌금을 부과하였다. 해당 DPO는 DPO로서의 업무를 수행하면서 개인정보 처리의 목적과 방법을 결정하는 업무를 수행하였기 때문에 GDPR이 금지하고 있는 직무의 이해충돌이 있다고 본 것이다. 이 사건은 개인정보 유출사건이 발생하여 감독기관에서 이를 조사하던 중, DPO가 이해충돌이 있는 업무를 동시에 수행하고 있음을 확인하고 벌금을 부과한 것이다. 해당 DPO는 DPO의 역할을 수행하면서 해당 기업에서 감사, 위험관리와 법 준수에 대하여 책임을 지는 이사였다. 따라서 불가피하게 이러한 부서의 개인정보 처리의 목적과 수단을 결정할 수밖에 없었던 것이다[362].
- 독일에서도 Bavarian Data Protection Authority가 DPO와 IT 매니저를 겸임한 경우에 DPO의 이해충돌 직무수행 금지를 위반한 것으로 보고 벌금을 부과한 사례가 있다[363].

여덟째, 기밀보호 의무이다. DPO는 유럽연합이나 회원국 법률에 따라 업무 수행에 관한 기밀보호 의무를 준수해야 한다[364].

바. DPO의 업무

DPO는 적어도 다음 업무를 맡아야 하고, 업무를 수행하면서 처리의 성격, 범위, 맥락 및 목적을 감안하여 처리 작업과 연관되는 위험을 충분히 고려해야 한다. 첫째, 정보와 조언 제공이다. DPO는 정보처리를 하는 자들(컨트롤러 또는 프로세서 및 그 종업원)에게 자신들의 의무에 대한 정보와 조언 제공을 하는 업무를 담당한다[365]. DPO는 구체적인 집행의 업무를 수행하는 것이 아니라, GDPR과 그 밖의 유럽연합 또는 회원국 개인정보 보호 규정에 따른 해당자의 의무가 무엇인지를 알려주고, 그에 따른 정보처리를 할 수 있도록 조언을 해 주는 역할을 담당하는 것이다.

<https://www.dataguidance.com/opinion/germany-role-dpo-and-conflicts-interest>.

362) JDSUPRA, 2020.8.11., “DPO and conflicts of interest within the company. DPO beware!”, <https://www.jdsupra.com/legalnews/dpo-and-conflicts-of-interest-within-57253/>.

363) Global Compliance News reports, 2016.11.22., “German company fined for DPO conflict of interest”, <https://iapp.org/news/a/german-company-fined-for-dpo-conflict-of-interest/>.

364) 제38조 제5항

365) 제39조 제1항 (a)

둘째, 모니터링과 감사, 교육이다. DPO는 법 준수에 대하여 모니터링을 수행한다. 즉, GDPR과 유럽연합 또는 회원국 개인정보 보호 규정, 개인정보 보호 관련 정책을 준수하는지 여부를 모니터링하고 감사를 해야 한다. 그리고 처리작업에 관여하는 직원의 책임을 할당하고, 인식 제고 및 교육도 수행한다[366].

셋째, 개인정보보호 영향평가에 관한 조언 제공이다. 이는 요청을 받은 경우의 업무이다. 개인정보보호 영향평가 수행에 대해서도 모니터링을 하는 업무를 수행해야 한다[367].

넷째, 감독기관과의 협력과 연락 업무이다[368]. 감독기관과의 연락은 정보처리 관련 문제에 대해서 감독기관의 연락 창구로 기능하는 것인데, 예를 들어 개인정보보호 영향평가와 관련해서 감독기관과 사전 협의를 하는 것이 여기에 해당한다[369]. 즉, 감독기관은 컨트롤러의 DPO와 사전 협의를 진행하게 된다. 그 외에도 감독기관과 협의를 하는 경우가 있다.

한편 DPO는 위험기반 접근의 방식(risk-based approach)으로 업무를 수행해야 한다. 그래서 GDPR은 DPO는 업무를 수행하면서 처리의 성격, 범위, 맥락 및 목적을 감안하여 처리 작업과 연관되는 위험을 충분히 고려해야 한다는 규정을 두고 있다[370]. 또한 GDPR은 컨트롤러나 프로세서에게 개인정보 처리에 관한 기록 보존의 의무를 부과하고 있는데, 이와 관련하여 DPO가 실질적으로 기록 보존을 하여야 할 경우도 있을 것이다[371].

사. 구체적인 실태

유럽연합에서 GDPR이 DPO의 선임 규정을 도입한 후, 유럽연합에서 DPO가 28,000명 정도, 미국과 전 세계에서는 약 75,000명이 필요할 것이라는 예측도 있었다[372]. 프랑스의 감독기관인 CNIL은 2018년 연차보고서(2019. 4. 15.)를 통해서 GDPR 시행 후 51,000개

366) 제39조 제1항 (b)
367) 제39조 제1항 (c)
368) 제39조 제1항 (d)
369) 제39조 제1항 (e)
370) 제39조 제2항
371) ARTICLE 29 DATA PROTECTION WORKING PARTY(2017c), op. cit., p19.
372) REUTERS, 2018.2.15., “Rise of the data protection officer, the hottest tech ticket in town”, <https://www.reuters.com/article/us-cyber-gdpr-dpo/rise-of-the-data-protection-officer-the-hottest-tech-ticket-in-town-idUSKCN1FY1MY>.

조직이 DPO를 채택하여 17,000명의 DPO가 선출되었다고 한다. 그 중 16,000개는 공공기관이라고 한다. 이와 같이 독립적이고 전문적인 DPO 직업군의 등장은 소위 풀링 효과(pooling effect)를 나타낸다고 평가하였다. CNIL은 2개의 DPO 자격 표준(certification standards) 승인했다. 현재 유럽연합에는 각국별로 DPO의 협회가 조직되어 있다.[373]

3. 우리나라 개인정보 보호법의 개인정보 보호책임자

가. 개인정보 보호법의 개인정보 보호책임자 지정 규정

우리나라 개인정보 보호법에는 개인정보 보호책임자 규정이 있는데, 해당 직책은 개인정보 처리 업무를 수행하는 담당자를 의미한다. 이는 GDPR에서 DPO가 수행할 업무와 이해충돌이 있는 개인정보 처리에 대한 수단과 방법을 결정하는 업무 담당자를 의미한다. 이와 같은 업무를 담당하는 자가 독립성을 가지고 개인정보 보호에 대한 모니터링과 조언 등을 수행할 수는 없다.

따라서 우리나라의 개인정보 보호법은 개인정보 처리 업무를 수행하는 책임자를 지정하라는 규정이다. 즉, 공공기관이나 기업에서 개인정보의 처리와 보호 등에 관한 업무를 총괄하여 담당하는 총괄 책임자로 속칭 CPO(Chief Privacy Officer)나 CSO(Chief Security Officer)로 지칭되는 직무를 담당하는 자를 지정하라는 것이다. 그런 관점에서 우리나라 개인정보 보호법의 개인정보 보호책임자 규정은 개인정보 처리 업무를 담당하는 담당자를 일정한 직급 이상의 자로 지정하도록 하고 담당 업무를 법률로 정하고 있다는 의미

373) 각국별 조직은 다음과 같다.
Austria - ARGE DATEN, Czech Republic - Spolek pro ochranu osobnch daj, Estonia - Eesti Andmekaitseliit, France - AFCP - Association Franaise des Correspondants la Protection des Donnes Caractre Personnel, Germany - GDD - Gesellschaft fr Datenschutz und Datensicherheit, Greece - HADPP - Hellenic Association of Data Protection & Privacy, Italy - ASSO DPO - Associazione data Protection Officer, Ireland - ADPO - The Association of Data Protection Officers Ireland, Luxembourg - APDL - Association pour la Protection des Donnes au Luxembourg, Netherlands - NGFG - Nederlands Genootschap van Functionarissen voor de Gegevensbescherming, Poland - SABI - Stowarzyszenie Administratorw Bezpieczestwa Informacji, Portugal- AEPD - Associa豫o de Encarregados de Prote豫o de Dados, Spain - APEP - Asociacin Profesional Espaola de Privacidad
Sweden - Forum fr Dataskydd, UK - NADPO - The National Association of Data Protection and Freedom of Information Officers

를 가질 뿐이다.

나. 개인정보 보호책임자의 업무

개인정보 보호법은 개인정보 보호책임자의 업무를 규정하고 있는데(제31조), 그 내용을 보면 개인정보 처리 업무를 총괄하여 수행하는 직위 즉, CPO(Chief Privacy Officer)와 CSO(Chief Security Officer)에 해당하는 직위로 볼 수 있다. 즉, 개인정보 보호책임자의 업무는 개인정보 보호 계획을 수립 및 시행하고, 개인정보 보호법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행 업무도 수행하며, 개인정보파일의 보호 및 관리, 감독 업무도 수행해야 하고, 개인정보 보호 관련 자료의 관리 업무, 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 업무도 수행해야 한다. 이 업무들은 해당 공공기관이나 기업에서 개인정보를 직접 처리하는 업무에 해당하고, 개인정보 처리의 목적과 방법을 결정하는 역할이다. 뿐만 아니라 개인정보 보호 수단은 어떻게 할 것인지를 선택하고, 그 집행을 총괄하는 업무를 담당하는 직위이다. 그 외에도 우리 개인정보 보호법이 개인정보 보호책임자의 업무로 규정한 업무들인 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선, 개인정보 처리와 관련한 불만의 처리 및 피해 구제, 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축 등의 업무 등이 있는데, 이런 것들도 모두 개인정보 처리와 직접 관련된 업무들이다. 따라서 이런 업무를 수행하는 개인정보 보호책임자는 GDPR에서 규정하는 DPO와는 이행충돌이 있는 직무를 수행하는 자에 해당한다.

다. 개인정보 보호법 상 개인정보 보호책임자의 독립성

개인정보 보호법에서 규정하고 있는 개인정보 보호책임자의 업무를 수행하는 자는 해당 업무에 대하여 독립성을 가지고 감독한다거나, 법률 규정에 부합하는지 여부를 조언하거나 정보를 제공하는 역할을 동시에 수행한다는 것이 모순될 수 밖에 없다. 즉, 업무에서 이해충돌이 발생하기 때문에 두 가지 업무를 독립적으로 수행하는 것을 기대할 수 없는 것이다. 개인정보 보호법은 개인정보 보호책임자가 위의 업무들을 수행함에 있어서 외부의 누구로부터도 지시를 받지 않고 독립적으로 수행할 수 있도록 보장하라는 규정도 두고 있지 않다. 실제로 개인정보의 수집 목적, 제3자 제공의 범위, 개인정보 보호조치의

수단과 방법 등을 규정하는 개인정보 처리방침은 기업이 사업 활동 목적에 맞게 방침을 결정해야 하는 것인데, 이 업무를 개인정보 보호책임자가 맡아서 수행할 때 개인정보 보호책임자에게 기업이 일체 관여하거나 지시할 수 없게 규율할 수는 없는 것이다.

개인정보 보호법이 규정하는 업무들과 감독 및 조언 등의 업무는 이해 충돌이 발생할 수 밖에 없다. 우리나라 개인정보 보호법에서 규정하고 있는 업무 중에서는 개인정보 보호 교육 계획의 수립 및 시행 정도만이 유일하게 개인정보 보호책임자의 업무로서 독립적으로 실행될 수도 있는 업무로 분류될 수 있을 것이다.

라. 조사, 보고, 개선조치

개인정보 보호법은 개인정보 보호책임자가 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등을 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다는 규정을 두고 있다. 그런데 앞에서도 본 바와 같이 개인정보 보호책임자가 담당하는 업무가 개인정보 처리에 대한 최고 책임자라고 한다면, 법령에서 조사나 보고를 받을 수 있다는 규정을 두고 있지 않더라도 주어질 것으로 보인다. 한편, 개인정보 보호법에는 개인정보 보호책임자가 개인정보 보호와 관련하여 법령 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다는 규정이 있는데, 이것도 개인정보 처리와 보호 등에 대한 업무를 총괄하는 직위에 있다면 당연한 규정을 부연한 것으로 볼 수 있다.

마. 불이익 금지

개인정보 보호법은 개인정보처리자는 개인정보 보호책임자가 각 업무를 수행함에 있어서 정당한 이유 없이 불이익을 주거나 받게 하여서는 아니 된다(제31조)고 규정하고 있는데 해당 규정은 큰 의미가 있다고 보기는 어렵다.

바. 개인정보 보호책임자를 선임해야 하는 경우

우리나라 개인정보 보호법은 GDPR과는 달리 모든 개인정보처리자에게 개인정보 보호

책임자를 지정할 의무를 부과하고 있다(제31조 제1항). 그러나 개인정보 보호책임자는 개인정보의 처리에 관한 업무를 총괄해서 책임진다는 의미 외에는 특별한 의미가 없다. 이와 같이 우리나라 개인정보 보호법에서 개인정보 보호책임자는 개인정보 처리 업무를 담당하는 자를 의미하기 때문에, 모든 개인정보처리자에게 개인정보 보호책임자를 두도록 규정하고 있어도 이 규정이 개인정보처리자에게 특별한 부담을 주지는 않을 것이다.

사. 개인정보 보호책임자의 지정요건

우리 개인정보 보호법은 개인정보 보호책임자의 자격에 대해서 전문성이나 법률적 지식 등에 대해서는 아무런 규정도 두고 있지 않다. 특정 자격을 갖추고 인증을 받은 자이어야 한다는 등의 규정이 없다. 단지 직위에 대한 규율만 하고 있을 뿐이다. 모든 개인정보처리자에게 개인정보 보호책임자를 지정하도록 하고 있기 때문에, 특별한 자격을 갖춘 자를 개인정보 보호책임자로 지정해야 한다는 규정을 두기 어려운 것도 있다.

우리 개인정보 보호법은 공공기관의 경우는 중앙행정기관은 고위공무원 또는 그에 상당하는 공무원, 각 시도는 3급 이상의 공무원과 같이 공무원의 직급을 규정하고 있을 뿐이다[374]. 공공기관 외의 개인정보처리자의 경우는 사업주 또는 대표자나 임원, 임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장을 개인정보 보호책임자로 지정하도록 규정하고 있다. 단, 개인정보처리자가 「소상공인 보호 및 지원에 관한 법률」 제2조에 따른 소상공인에 해당하는 경우에는 별도의 지정 없이 그 사업주 또는 대표자를 개인정보 보호책임자로 지정한 것으로 본다는 규정을 두고 있다. 한편, 이 경우에도 개인정보처리자가 별도로 개인정보 보호책임자를 지정할 수 있다(시행령 제32조 제

374) 예를 들어, 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관은 고위공무원단에 속하는 공무원(이하 "고위공무원"이라 한다) 또는 그에 상당하는 공무원, 그 외 정무직공무원을 장(長)으로 하는 국가기관은 3급 이상 공무원(고위공무원을 포함한다) 또는 그에 상당하는 공무원, 그 외에 고위공무원, 3급 공무원 또는 그에 상당하는 공무원 이상의 공무원을 장으로 하는 국가기관은 4급 이상 공무원 또는 그에 상당하는 공무원, 그 외의 국가기관(소속 기관을 포함한다)은 해당 기관의 개인정보 처리 관련 업무를 담당하는 부서의 장, 시·도 및 시·도 교육청은 3급 이상 공무원 또는 그에 상당하는 공무원, 시·군 및 자치구는 4급 공무원 또는 그에 상당하는 공무원, 각급 학교는 해당 학교의 행정사무를 총괄하는 사람, 그 외의 공공기관은 개인정보 처리 관련 업무를 담당하는 부서의 장. 다만, 개인정보 처리 관련 업무를 담당하는 부서의 장이 2명 이상인 경우에는 해당 공공기관의 장이 지명하는 부서의 장이 된다는 식으로 직급만을 규정하고 있다.

2항 제2호).

4. 개인정보 보호법 개선방안 : DPO 도입

가. 개인정보 처리 집행 업무를 담당하지 않으면서 독립적으로 업무를 수행할 수 있는 DPO 도입

우리 개인정보 보호법에서도 CPO에 해당하는 '개인정보 보호책임자' 아니라, 독립적인 지위에서 감독과 조언 및 정보제공을 할 수 있는 '독립 정보보호 책임자(DPO)'를 도입할 필요가 있다. 이 경우 기존의 개인정보 보호책임자 규정은 폐지하고, DPO를 신설하는 것이 바람직할 것이다. CPO에 해당하는 개인정보 보호책임자는 굳이 개인정보 보호법에 규정하지 않아도 기업에서는 당연히 선임하는 직책이기 때문이다.

나. 지정 요건

DPO를 선임하도록 의무를 도입한다면, 이를 모든 기업에게 선임 의무를 부과하는 것보다는 위험성이 높은 방식으로 개인정보를 처리하거나, 위험성이 높은 개인정보를 처리하는 경우에만 선임할 의무를 부과하는 것이 바람직할 것이다. GDPR의 경우와 같이, 개인정보처리자의 핵심 활동(core activities)이 정보주체에 대한 대규모의 정기적, 체계적 모니터링을 필요로 하는 처리 작업으로 구성되는 경우로 규정할 수도 있을 것이다. 개인정보 처리와 관련된 업무를 수행하는 자가 아닌 독립적 지위에서 감사 등의 업무를 수행하는 직책이므로 매우 작은 규모의 기업이나, 개인정보 처리가 주된 업무가 아닌 기업에는 선임을 의무화할 필요는 없을 것이다. 반면, 공공기관이나 공적 업무를 수행하는 조직인 경우는 규모와 관련 없이 선임의 필요성이 있다. 다만, 이 경우는 여러 조직을 통합하여 DPO가 지정될 수 있게 할 수 있다. 기업의 경우에도 다수의 계열사를 포괄하여 단일한 DPO를 지정할 수 있도록 허용할 수 있을 것이다.

다. 자격 요건과 자격 인증기관

DPO는 전문성을 갖는 자로 선임하도록 할 필요가 있고, 그에 대한 자격증과 인증기관에 대한 규정도 마련하는 것이 좋을 것이다. 이와 관련해서는 현재의 CPO 포럼과 같이 개인정보처리자를 회원으로 하고 CPO들의 협의체와 같은 성격을 갖는 조직은 독립성을 가진 것으로 보기 어려우므로, 이들을 통해서 자격 및 인증 업무를 수행하는 것은 바람직하지 않다. DPO들이 구성하는 협회 등을 통해서 해당 업무가 이루어질 수 있도록 할 필요가 있다.

라. 지위와 업무

DPO 제도를 도입한다면, DPO의 지위와 관련해서는 (i) 관여 보장 - 개인정보 보호와 관련한 모든 문제에, 적시에 적절한 방식으로 관여할 수 있도록 보장하고. (ii) 필요한 자원 제공과 지원의무 - DPO가 업무를 수행할 수 있도록 해당 업무와 개인정보 및 처리작업에 대한 접근을 수행하고, 전문지식을 유지하는 데 필요한 자원을 제공하여 DPO를 지원하도록 해야 한다. 또한 (iii) 지시 금지 보장, (iv) 불이익 금지. (v) 직접 보고. (vi) 정보주체의 연락가능성. (vii) 이해충돌 금지, (viii) 기밀보호 의무 등을 규정할 필요가 있다.

그 업무로는 (i) 정보와 조언 제공 - 정보처리를 하는 자들에게 자신들의 의무에 대한 정보와 조언 제공, (ii) 모니터링과 감사, 교육, (iii) 개인정보 영향평가에 관한 조언 제공, (iv) 감독기관과의 협력과 연락 업무 등을 규정할 수 있다.

제9절 개인정보 보호 행동강령과 인증 등과 관련하여 자율규제의 촉진과 그 조건

1. 개요

개인정보 보호와 관련하여 개인정보처리자의 자율규제를 촉진하고, 그 방법으로 인증을 활성화하는 것은 오랫동안 각국에서 추진되어 온 정책이다. GDPR은 여러 개의 조문을 신설하여 개인정보 보호와 관련한 행동강령과 인증제도에 대한 규정을 두고 있다(제5절)[375]. 이는 행동강령과 인증제도를 통해서 각 부문별 특수성을 가진 개인정보 처리와 관련하여 해당 부문의 특수성을 반영하는 규율을 구체화하고, 이를 행동강령의 승인과 인증이라는 제도를 통해서 각 부문별로 자율적인 규제를 활성화하고, 감독과 권리구제의 실효성을 높이기 위한 것이다. 아울러 영세 및 중소규모의 기업(micro, small and medium sized enterprises)의 특수한 필요성도 고려하기 위함이다[376]. 그런데 이와 관련하여 GDPR은 자율규제의 전제로 행위규범에 대한 감독기관의 사전, 사후 통제 및 승인과 전문성을 갖추고 독립성이 보장되는 구체적인 감독 권한을 가지면서 인증 위반에 대해서 지속적인 모니터링을 할 수 있는 기관인 인증기관의 존재를 전제하고 있다. 아울러 행동강령에는 권리구제도 포함하도록 하고 있어서, 승인된 행동강령과 독립적인 인증기관은 독립성을 갖는 권리구제 제도로서도 역할을 할 수 있도록 하고 있다. 또한 GDPR은 국제표준제도(ISO)와의 연계까지도 규정하고 있다.

유럽연합은 각 부문별 승인된 행동강령의 활성화와 자율규제에 대해서 많은 기대를 하고 있는데, 2020년 9월에는 최초로 스페인 개인정보 감독기관(Spanish Supervisory Authority, AEPD)에 의해 광고에서 개인정보 처리와 관련한 행동강령(Code of Conduct for Data Processing in Advertising)이 승인[377]되었다[378]. 이 행동강령은 스페인의 광고

375) GDPR 제5절은 행동강령과 인증이라는 제목으로, 제40조 행동강령, 제41조 승인된 행동강령 모니터링, 제42조 인증, 제43조 인증단체에 대한 4개의 조문을 두고 있다.
376) 제40조 제1항
377) AEPD의 승인 결정문.
<https://www.aepd.es/sites/default/files/2020-11/resoluci%C3%B3n-aprobacion-CC.0004.2018-AUTOCONTROL.pdf>.
378) AEPD의 GDPR 행동강령에 대한 FAQ는 여기에서 참고할 수 있다.
<https://www.insideprivacy.com/data-privacy/the-spanish-supervisory-authority-appr

산업과 관련한 자율규제 감독기관으로 비영리 협회인 AUTOCONTROL(Asociacin para la Autorregulacin de la Comunicacin Comercial)에 의하여 제정된 것이고, 이를 감독할 기관은 Advertising Jury(Jurado de la Publicidad)이다. 현재 많은 부문에서 부문별 행동강령을 승인받기 위한 준비를 하고 있다고 한다.

한편, 우리나라에도 개인정보 보호법과 정보통신망법 등에는 개인정보 보호나 정보보호에 대한 인증제도가 있는데, 법률상의 의무로 규정된 것이어서 사실상 정부에서 주도하는 것으로 각 분야의 자율규제를 촉진하는 역할은 제한적이다. 우리나라에서도 독립성과 감독 권한 및 권리구제 등 실행력이 있는 모니터링 기관을 갖추고, 개인정보 보호법과 조응하는 행동강령을 개인정보 보호위원회가 승인하는 제도를 도입하는 것이 바람직할 것이다.

2. 개인정보 보호 영역에서의 자율규제와 GDPR의 행동강령과 인증에 대한 규정

가. 개인정보 보호 영역에서의 자율규제

개인정보 보호는 기술 발전이 매우 빠른 영역이기 때문에 자율규제나 새로운 방식의 규율이 필요하다는 논의는 꾸준히 제기되어 왔다. 예를 들어 로렌스 레식(Lawrence Lessig)은 기술은 프라이버시 규율의 새로운 모델을 만들어낼 것이라고 주장하였다[379].

개인정보 보호에서의 자율규제는 경제주체나 사회적 파트너, 비영리 민간단체나 협회 등이 스스로 공동의 가이드라인을 채택하는 기회를 갖는 것으로 정의하거나[380], 프라이버시 보장을 이해관계자에 기반한 모델로 정의한다[381]. 통상 자율규제는 규칙 제정, 규칙의 집행, 판단의 영역으로 나누어 세 가지 모두 또는 그 중 하나라도 이해관계자에 기반하여 이루어지는 것을 말한다고 한다. 규칙의 제정은 누가 개인정보 보호의 규칙을 정하

---

oves-a-gdpr-code-of-conduct-on-advertising/>.

379) Lawrence Lessig: Technology Will Create New Models for Privacy Regulation. The Wall Street Journal. <https://www.wsj.com/articles/BL-CIOB-8802>

380) European Commission(2003), European Parliament & Council of Ministers (2003), Inter-Institutional Agreement on Better Lawmaking, p1.

381) IAPP, “Self-Regulation Model”, <https://iapp.org/resources/article/self-regulatory-model/>

는가인데, 자율규제에서는 이를 기업, 사업자협회 등에서 정한다. 규칙의 집행은 누가 규칙의 집행을 하는가인데, 개인정보 감독기관이 하거나, 정부 기관, 또는 협회의 행동강령 집행기관에서 할 수도 있다. 판단은 규칙을 위반했는지 여부를 판단하는 것을 말한다[382]. 이런 점에서 자율규제에는 순수한 자율규제의 모델에서부터 공동 규율 모델까지 여러 가지 유형의 자율규제 유형이 있다.

나. 행동강령에 대한 GDPR의 규정

1) 행동강령 수립 장려와 특정 분야 협회의 행동강령

GDPR은 다양한 처리 분야의 특성을 고려한 GDPR의 적절한 적용에 기여하기 위해서 분야별 행동강령이 마련되는 것을 장려하고 있다. 그리고 초소형기업 및 중소기업의 특수한 요구사항을 고려한 규정의 적절한 적용도 아울러 행동강령 수립을 장려하는 이유로 꼽고 있다[383]. GDPR은 컨트롤러나 프로세서 범주를 대표하는 협회와 그 밖의 단체를 해당 범주의 개인정보 처리와 관련한 특성을 고려하여 GDPR을 적절하게 적용할 수 있는 구체화된 행동강령을 수립하는 주체로 예정하면서, 이 경우 행동강령에서 구체화할 내용을 적시하고 있는데, 해당 행동강령을 모두 준수한다고 해서 GDPR의 완전한 준수를 보증하는 것은 아니므로 해당 내용은 예시적인 내용이 될 것이다.

특정 분야 협회의 행동강령(제40조 제2항)에는 (a) 공정하고 투명한 처리의 원칙, (b) 특정 맥락에서 컨트롤러가 추구하는 정당한 이익에 대한 판단, (c) 개인정보 수집과 관련한 행동강령, (d) 개인정보 가명화에 대한 규정, (e) 일반 대중과 정보 주체에게 제공되는 정보, (f) 정보 주체의 권리 행사, (g) 어린이에게 제공되는 정보, 어린이에 대한 보호, 어린이의 친권자 동의를 구하는 방식, (h) 컨트롤러가 책임성을 준수하기 위해 취할 기술적, 조직적 조치, 설계에 의한 개인정보 보호, 기본설정에 의한 개인정보 보호를 위한 조치, 개인정보 보호와 관련하여 보안을 보장하기 위해 필요한 조치, (i) 감독기관에 대한 개인정보 침해 통지, 정보 주체에 대한 개인정보 침해 통지, (j) 제3국이나 국제기구로의 개인정보 이전, (k) 정보 처리와 관련한 컨트롤러와 정보주체 간 분쟁을 해결하기 위한

382) Ibid.
383) 전문 98, 제40조 제1항

법정 밖에서의 절차 및 기타 분쟁 해결 절차(단, 이 절차로 인해서 정보 주체의 분쟁해결에 대한 권리에는 영향을 미치지 않음) 등이 포함된다.

아울러 GDPR은 행동강령이 감독기관에 의해서 승인될 경우 제3국이나 국제기구로의 개인정보 이전과 관련하여 적절한 보호조치로도 기능할 수 있도록 규정하고 있다. 이런 점에서 승인된 행동강령은 개인정보의 제3국이나 국제기구로의 이전과 관련한 하나의 적법성 보증 수단이 될 수 있고, 유럽연합 외부 제3국에서 승인된 행동강령을 인증받는 것이 효용을 가질 수 있을 것이다.

2) 특정 분야 협회의 행동강령 승인 절차와 승인된 행동강령의 공표와 등록

GDPR은 감독기관로부터 '승인된 행동강령'이 되어야 여러 가지 효과를 인정하고 있다. 특정 분야 협회의 행동강령의 승인 절차는 개인정보 감독기관과 의견 조율을 거쳐 이루어진다. 감독기관으로부터 적절한 보호장치를 제공하여 GDPR에 부합한다는 승인을 받아야 한다. 이 과정에서 협회는 감독기관과 의견을 나눌 수 있고, 초안에 대한 감독기관의 의견을 들을 수 있다. 해당 협회나 단체는 행동강령을 마련할 때와 이를 개정하거나 확대할 때 감독기관에 규범 초안이나 개정안, 확대안을 제출하고 의견을 조율하는 과정을 거치도록 하고 있다. 감독기관은 규범 초안이나 개정안 또는 확대안을 승인할 경우, 이를 등록하고 공표해야 한다 해당 행동강령이 여러 나라에서의 처리 활동과 관련된 것일 때에는 EDPB에 제출하고 부합 여부에 대한 EDPB의 의견을 들어야 한다. 이 경우 집행위원회가 유럽연합 내에서 일반적 유효성을 갖는다고 결정할 수 있다. EDPB는 승인된 행동강령과 개정본 및 확대본 모두를 등록부에 수록하고 적절한 수단을 통해 공중이 이에 접근할 수 있도록 해야 한다.

3) 특정 분야 협회의 행동강령 준수 여부를 모니터링하고 권리구제를 하는 기관

GDPR의 행동강령에 대한 규정에서 특징적인 것은 행동강령에는 반드시 전문성을 갖고 독립성이 보장되는 모니터링 기관을 두도록 하고 있다는 점이다.[384] 이 모니터링 기관은 권리구제 기능까지도 수행하게 된다. 이는 자율규제의 실효성을 담보하는 매우 중

384) 제41조

요한 전제가 된다.

특정 분야 협회의 행동강령에는 모니터링 기관에서 행동강령 준수를 약속한 컨트롤러나 프로세서의 준수 여부를 의무적으로 모니터링을 수행할 수 있게 하는 메커니즘이 포함되어 있어야 한다. 물론 이 경우에도 감독기관에 의한 감독업무나 권한은 영향을 받지 않는다. 이와 같은 모니터링 업무는 감독기관으로부터 행동강령 준수 모니터링 단체로 인가를 받은 단체에 의해서 수행되어야 하는데, 해당 단체는 다음과 같은 조건을 갖추고 있어야 한다.

첫째, 독립성과 전문성. 즉, 단체의 독립성과 행동강령의 주제와관련한 전문성을 주무 감독기관이 만족할 만한 수준으로 입증해야 한다.

둘째, 모니터링 절차 수립. 관련 컨트롤러나 처리자의 규범 적용 적격성을 평가하고, 관련 조항 준수를 모니터링하고, 처리 작업을 주기적으로 검토할 수 있는 절차를 수립해야 한다.

셋째, 민원 처리 절차 수립. 행동강령의 위반 또는 행동강령 이행 방식(과거 또는 현재)에 대한 민원을 처리하기 위한 절차 및 구조 수립, 그리고 해당 절차 및 구조를 정보주체와 일반 대중에게 투명하게 공개하기 위한 절차 및 구조를 수립해야 한다.

넷째, 이해충돌 방지. 해당 단체의 업무와 임무가 이해충돌을 일으키지 않음을 주무 감독기관이 만족할 만한 수준으로 입증해야 한다.

한편 모니터링 단체는 컨트롤러나 프로세서가 행동강령을 위반한 경우에는 해당 행동강령에서 위반 컨트롤러나 프로세서를 배제하거나 정지시키는 등 적절한 조치를 취하고 이를 감독기관에 알려야 한다. 감독기관은 모니터링 단체가 인가 조건이 충족되지 않게 되거나 부적절한 행위를 하는 경우 인가를 취소한다.

4) 행동강령 제정과 개정 과정에서 정보주체나 이해당사자들의 의견 수렴

GDPR 전문에서는 행동강령을 제정하거나 개정할 때, 특정 분야의 컨트롤러나 프로세서들을 대표하는 협회나 기관들은 적절한 이해관계자들과 개인정보주체들과 협의해야 하고, 그러한 협의에서 제시된 제안과 견해를 유념해야 한다는 규정을 두고 있다[385].

385) 전문 99

다. 인증

1) 목적

개인정보 보호 인증 메커니즘 혹은 인장과 마크는 컨트롤러나 프로세서에 의한 처리 작업이 GDPR을 준수한다는 것을 입증하기 위한 목적으로 도입되었다. 이와 관련해서도 초소형기업과 중소기업의 특수한 요구가 고려될 수 있도록 하고 있다.[386] 아울러 인증 메커니즘과 인장 및 마크는 제3국이나 국제기구로의 개인정보 이전 체계에서 적절한 보호장치로 인정될 수도 있다. 단 이 경우 해당 컨트롤러와 프로세서는 계약 또는 기타 법적 구속력이 있는 문서를 통해 정보주체의 권리와 관련한 것을 포함해 그러한 적절한 보호조치를 적용하겠다는 구속력 있고 집행 가능한 약속을 해야 한다.

2) 인증의 역할

인증은 승인된 인증단체가 감독기관에서 승인한 기준을 바탕으로 발급되어야 하는데, 인증은 자발적인 것이고 GDPR 규정을 준수해야 할 컨트롤러나 프로세서의 책임을 감경하는 것은 아니다. 그리고 인증은 감독기관의 감독 업무나 권한에도 영향을 미치지 않는다. 한편, EDPB가 인증 기준을 승인한 경우는 공통 인증인 유럽 정보보호 인장(European Data Protection Seal)이 될 수 있다.

인증 메커니즘에 처리(정보)를 제출하는 컨트롤러나 프로세서는 해당하는 경우 제43조의 인증기관 또는 주무 감독기관에 인증 절차 수행에 필요한 모든 정보와 처리 활동에 대한 접근권을 제공해야 한다. 컨트롤러나 프로세서에 대한 인증은 최대 3년의 기간에 대해 발급되고, 관련 요구사항이 계속 충족되는 것을 전제로 동일한 조건으로 갱신될 수 있다. 인증을 위한 요구사항이 충족되지 않거나 더이상 충족되지 않게 된 경우, 인증기관 또는 주무 감독기관에 의해 인증이 철회된다. EDPB는 모든 인증 메커니즘과 인장 및 마크를 등록부에 수록하고 적절한 수단을 통해 공중이 이에 접근할 수 있도록 해야 한다.

386) 제42조

라. 인증기관

1) 인증기관

인증을 발급하고자 하는 인증기관은 개인정보 보호와 관련하여 적절한 수준의 전문성을 갖추어야 하고, 감독기관이나 유럽의회 및 이사회 규정(EC) No765/2008에 따라 지명된 국가 인가기관으로부터 인가를 받아야 한다. 이와 같은 인증기관에 의한 인증의 발급과 갱신은 주무 감독기관의 업무나 권한에는 영향을 미치지 않는다. 인증기관은 인증을 발급하거나 갱신하는 경우 감독기관에게 미리 알려야 한다. 인증기관은 인증이나 인증 철회를 초래하는 적절한 평가에 대해 책음을 져야 한다. 이는 컨트롤러나 프로세서가 GDPR 규정을 준수해야 할 의무에 영향을 미치지는 않는다.

2) 인증기관의 요건

인증기관이 갖추어야 할 요건은 다음과 같다. 첫째, 기관의 독립성과 인증의 주제 사안과 관련한 전문성을 주무 감독기관이 만족할 만한 수준으로 입증해야 한다. 둘째, 감독기관, EDPB가 승인한 기준으로서, 주무 권한을 가진 감독기관이 승인하거나 EDPB가 승인한 기준을 존중하겠다고 약속해야 한다. 셋째, 개인정보 보호 인증과 인장 및 마크의 발급, 주기적 검토 및 철회를 위한 절차를 수립해야 한다. 넷째, 인증 위반 또는 컨트롤러나 프로세서의 인증 이행 방식(과거 또는 현재)에 대한 민원을 처리하기 위한 절차 및 구조 수립, 그리고 해당 절차 및 구조를 정보 주체와 일반 대중에게 투명하게 공개하기 위한 절차 및 구조를 수립해야 한다. 다섯째. 해당 기관의 업무와 임무가 이해충돌을 일으키지 않음을 주무 감독기관이 만족할 만한 수준으로 입증해야 한다.

3) 인증의 기준

인증 기준은 쉽게 접근할 수 있는 형태로 감독기관에 의해 일반에 공개되어야 한다. 감독기관은 해당 요구사항 및 기준을 EDPB에 전송해야 한다. EDPB는 모든 인증 메커니즘과 개인정보 보호 인장을 등록부에 수록하고 적절한 수단을 통해 공중이 이에 접근할 수 있도록 해야 한다. 인증기관는 요청된 인증의 부여 또는 철회 사유를 주무 감독기관에 제공해야 한다.

4) 인가와 인가의 철회

인증기관에 대한 인가는 최대 5년의 기간에 대해 발급되고, 인증기관이 규정에 명시된 요구사항을 충족하는 것을 전제로 동일한 조건으로 갱신될 수 있다. 주무 감독기관이나 국가 인가기관은 인가 조건이 충족되지 않거나 더 이상 충족되지 않게 된 경우, 또는 인증기관이 취한 행동이 GDPR에 위배되는 경우 인증기관에 대한 인가를 철회할 수 있다.

3. 우리나라 개인정보 보호와 관련한 자율규제와 인증

가. 개요

우리나라의 개인정보 보호와 관련한 자율규제는 개인정보 보호법 제5조 제3항과 제13조에서 자율규제의 촉진과 지원에 대한 규정으로 그 근거를 마련해 두고 있고, 그에 따라서 자율규제 규약, 자율규제단체, 자율점검 등을 구체화하고 있다. 한편, 정보통신망법은 정보통신서비스 제공자단체의 이용자 보호를 위한 자율규제에 대한 규정을 두고 있으며[387], 그에 따라서 방송통신위원회는 2018년에 '방송·통신·온라인분야 개인정보 보호 자율규제 기본계획'을 수립하고 자율규제를 추진해 왔다. 한편, 우리나라 개인정보 보호 관련 인증제도는 법률에서 일정한 기준에 해당하는 사업자로 하여금 반드시 인증을 받도록 강제하고 있는 제도로서 도입되어 있다.

나. 우리나라의 개인정보 보호 관련 자율규제

1) 구속력이 없는 자율규제

개인정보 보호 업무가 개인정보 보호위원회로 이관되기 전의 우리나라의 개인정보 보호와 관련한 자율규제는 행정안전부와 방송통신위원회에서 주관하였다. 관련 근거 법률로는 개인정보 보호법 제5조 제3항과 제13조, 정보통신망법 제44조의 4이다. 그에 따라 행정안전부는 개인정보처리자의 자율적인 개인정보 보호 활동을 촉진하기 위해서 기관이

387) 정보통신망법 제44조의 4

나 단체에 필요한 지원을 할 수 있는 권한을 가지고 있었다(시행령 제14조). 현재는 개인정보 보호위원회가 자율규제에 대한 권한을 가지고 있다.

개인정보 보호법에 따른 자율규제는 개인정보 보호위원회 고시인 '개인정보보호 자율규제단체 지정 등에 관한 규정'[388]에 상세한 규정을 두고 있다. 방송통신위원회는 '방송·통신·온라인 분야 개인정보보호 자율규제 기본계획'을 수립하여 그에 따라 자율규제를 위한 정책을 추진했다. '개인정보보호 자율규제단체 지정 등에 관한 규정'에 의하면, '자율규제단체'를 통한 '자율규제 규약'의 제정과 '자율점검'이 핵심적 내용인데, 앞에서 본 GDPR의 자율규제와 관련한 승인된 행동강령이나 인증기관 및 인증과 큰 차이가 있다.

우리나라의 개인정보 보호법 상 자율규제 규약은 다음과 같은 특징이 있다. 첫째, 자율규제단체가 소속 개인정보처리자의 개인정보 처리 특성을 고려하여 개인정보 보호에 필요한 규약을 작성하고 공표하는 것인데[389], 원칙적으로 개인정보 보호법에 부응하는 것인지 여부와는 관련이 없다.

둘째, 자율규제 규약은 자율규제협의회가 검토하도록 하고 있으나, 자율규제협의회에게는 자율규제 규약에 대한 명시적인 권한이 없다[390]. 자율규제협의회는 개인정보 보호위원회, 자율규제단체 소관 행정기관, 전문기관 및 해당 분야 전문가로 구성하며 위원은 보호위원회, 자율규제단체 소관 행정기관 소속 개인정보 보호 업무를 담당하는 국장급 공무원, 한국인터넷진흥원의 개인정보 보호 업무를 담당하는 임직원, 개인정보 보호와 자율규제에 관하여 학식과 경험이 풍부한 전문가 5인 이내로 구성한다. 자율규제 규약은 개인정보 보호위원회와는 아무 상관이 없으며, 개인정보 보호법의 사전, 사후 검토 및 승인절차가 없다다. 따라서 해당 자율규제 규약이 개인정보 보호법에 부합해야 한다는 조건도 없다.

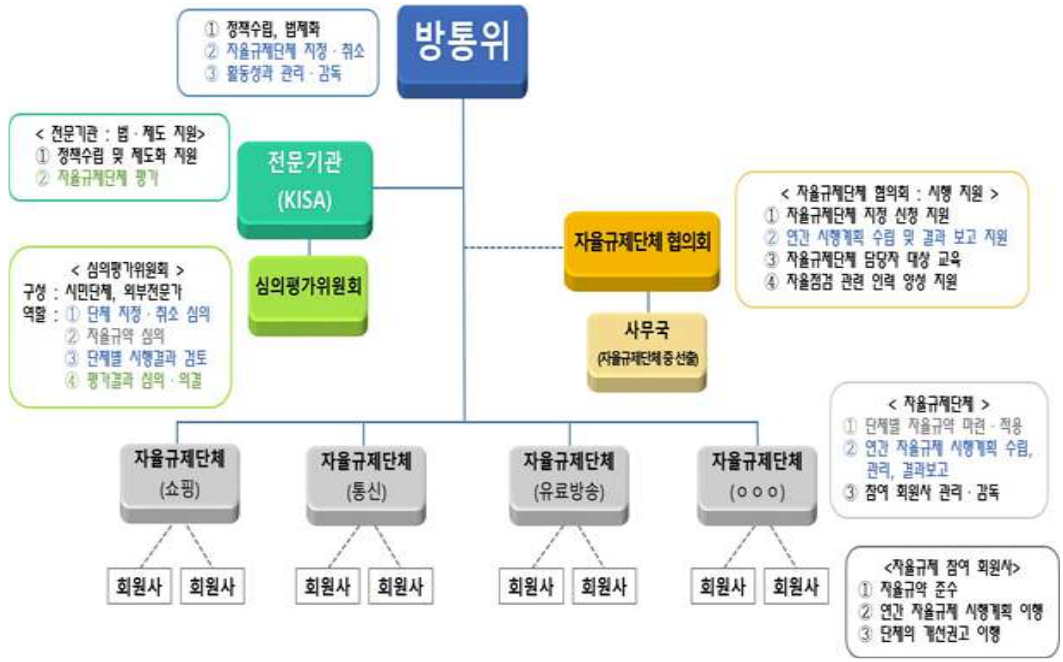
---

388) 이 규정이 제정된 2019년에는 행정안전부가 본 업무를 담당하였으므로 행정안전부령이었는데, 현재는 개인정보 보호위원회가 본 업무를 담당하게 되었으므로 향후 개인정보 보호위원회 고시로 제정될 것으로 보인다.

389) 개인정보보호 자율규제단체 지정 등에 관한 규정 제11조 제1항

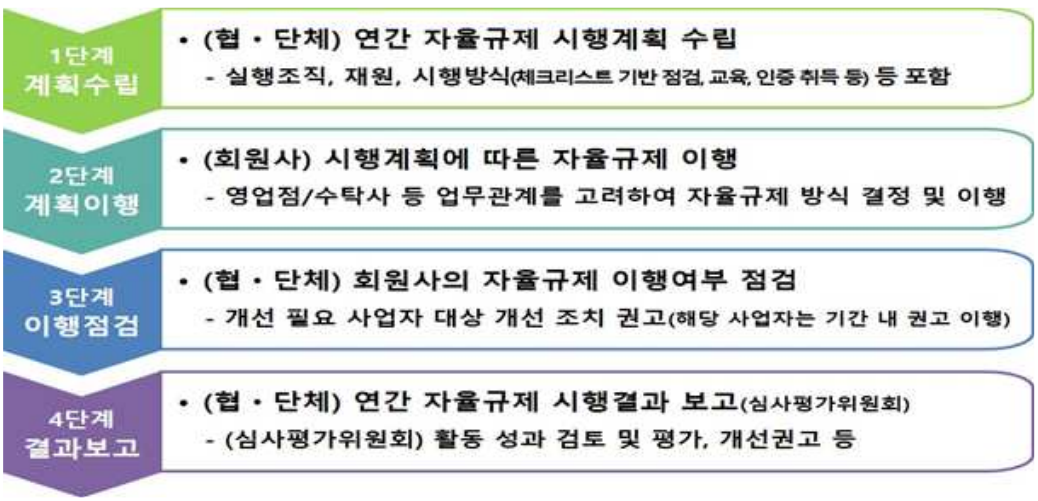
390) 자율규제협의회는 자율규제단체의 지정 및 지정 취소에 대한 심사, 자율규제 규약에 대한 검토, 연간 개인정보보호 수행계획 및 결과에 대한 검토, 개인정보보호 수행계획에 따른 결과의 평가에 대한 검토, 그 밖에 자율규제단체의 개인정보 보호 활동에 관하여 필요한 사항 등의 업무를 하는 조직이다.

<그림5-4> 방송통신위원회가 발표한 자율규제의 추진체계



*출처 : 방송통신위원회(2018)

<그림5-5> 개인정보보호 자율규제 시행절차



셋째, 협회에 소속된 개인정보처리자는 해당 규약을 준수할 의무도 없고, 자율규제 규약을 준수하도록 노력해야 한다는 규정만 있다[391]. 자율규제단체도 소속 개인정보처리자가 자율규제 규약을 준수하도록 지도, 권고 등 필요한 조치를 할 수 있을 뿐이다. 따라서 개인정보 감독기관의 승인을 얻어야 하는 GDPR의 승인된 행동강령과 차이가 있다. 현행 규정에 따르면 자율규제단체는 개인정보처리자를 회원사로 구성되는 협회나 단체인데, 자율규제단체로 지정되려면 자율규제단체 지정신청서와 연간수행계획을 협의회에 제출해서 심사를 받고 단체지정서를 발급받아야 한다. 자율규제단체는 소속 개인정보처리자의 자율적인 개인정보 보호 활동을 지원하기 위하여 교육, 홍보와 자율점검 등을 수행하게 된다.

넷째, 자율점검은 자율규제단체가 자율규제 규약에 따라 소속 개인정보처리자의 개인정보 처리 실태를 점검하고 미흡한 점을 개선하도록 지도하는 것을 말한다. 규정은 자율규제단체로 하여금 실태 점검 최소 1개월 전에 소속 개인정보처리자가 스스로 개인정보처리 실태를 점검할 수 있도록 표준 자율점검표를 마련하여 배포하여야 한다고 규정하고 있다. 즉, 자율점검은 강제력이 없는 개선지도를 의미한다. 단, 자율점검 시 개인정보 처리실태에 따른 개선을 지도받았음에도 불구하고 이를 이행하지 아니한 경우는 소속 자율규제단체에 참여할 수 없게 하는 불이익이 주어진다. 한편, 자율규제단체의 자율규제 활동에 참여하는 소속 개인정보처리자가 자율규제 규약을 충실히 준수하고 자율점검을 성실히 수행하여 수행 결과가 우수하다고 인정되는 경우에는 개인정보 보호위원회의 자료제출 요구 및 검사를 1년간 면제할 수 있다는 규정을 두고 있다.

2) 자율규제단체의 현황

개인정보 보호위원회에 의하여 지정된 자율규제단체는 아래와 같이 각 분야별로 구성되어 있다[392].

391) 개인정보보호 자율규제단체 지정 등에 관한 규정 제11조 제3항

392) 개인정보보호 자율규제 업무 소개 웹사이트에는 개인정보 보호위원회 주관으로 국민 생활과 밀접한 7개 분야 14개 자율규제 단체가 지정·운영되고 있으며 향후 다양한 분야에서 자율규제 단체 확대를 준비하고 있다고 소개하고 있다.

<표5-3> 개인정보보호위원회에 의하여 지정된 자율규제단체

구분	전문기관	협단체
총괄 전문기관	한국인터넷진흥원	대한병원협회, 한국여행업협회, 한국호텔협회, 한국렌터카사업조합연합회, 한국공인중개사협회, 한국학원총연합회, 한국골프장경영협회, 한국대중골프장협회
의약분야 전문기관	건강보험심사평가원	대한의사협회, 대한약사회, 대한한방병원협회, 대한치과의사협회, 대한한의사협회
복지분야 전문기관	한국사회보장정보원	한국노인종합복지관협회
통신 분야	한국인터넷진흥원	개인정보보호협회
쇼핑분야	한국인터넷진흥원	한국온라인쇼핑협회

* 한국온라인쇼핑협회, 한국정보통신진흥협회, 한국알뜰통신사업자협회, 한국게임산업협회, 한국CATV협회, 한국IPTV방송협회, 한국인터넷기업협회, 개인정보보호협회

다. 우리나라 자율규제의 현황과 개선방안

1) 구속력이 전혀 없는 자율규제에서 일정한 구속력을 갖춘 자율규제로

우리나라의 자율규제 단체는 자율규제 규약을 자율적으로 제정하는데, 해당 자율규제 규약이 개인정보 보호법에 조응하는 것인지 여부에 대한 판단을 받는 구조가 마련되어 있지 않다. 아울러 해당 단체에 소속된 개인정보처리자는 자율규제 규약을 준수할 의무도 없다. 게다가 자율규제 단체나 독립된 인증기관이 규약의 준수 여부를 모니터링하는 구조도 갖추고 있지 않다. 따라서 현재 우리나라의 자율규제는 아무런 구속력이 없는 순수한 자율규제의 유형으로 볼 수 있다. 그런데, 이러한 순수 자율규제의 유형보다는 자율규제 규약에 대한 승인 제도를 두고, 만약 승인된 자율규제 규약을 채택하여 개인정보 보호법 준수에 대한 외부적인 인증의 효과를 누릴 수 있도록 하려면, 자율규제 규약에 대한 승인절차를 두는 것이 좋을 것이다. 이 경우, 자율규제 규약이 개인정보 보호법에 부합하는지 여부를 개인정보 보호위원회에 승인을 신청하여 승인을 받을 수 있는 절차를 둘 필요가 있다. 개인정보 보호위원회는 해당 자율규제 규약이 개인정보 보호법에 비추어 타당하다고 인정되는 경우에는 승인을 하고 이를 공고하게 된다.

2) 공정성을 담보할 수 있는 독립적이고 전문적인 자율규제 모니터링 기관의 도입

현재 우리나라의 자율규제에는 공정성을 담보할 수 있는 독립적이고 전문적인 자율규제 모니터링 기관이 존재하지 않는다. 그런데 만약 자율규제 규약에 대해서 개인정보 보호위원회의 승인을 받도록 하고, 승인된 자율규제 규약의 준수 여부를 모니터링하여 이를 준수하는 개인정보처리자에 대하여 인증을 해 주는 절차를 도입한다면, 자율규제 규약의 준수 여부를 감독하고 모니터링할 수 있는 제도가 마련되어야 한다. 이 모니터링 기관은 해당 개인정보처리자로 구성된 협회나 단체 또는 해당 개인정보처리자로부터 독립성이 있어야 하고 전문성을 갖추어야 한다. 이 모니터링 기관에는 각 개인정보처리자에 대한 권리구제 신청 등에 대응하여 권리구제를 처리할 수 있는 권한도 부여되는 것이 좋다. 한편, 각 개인정보처리자가 자율규제 규약을 준수하지 않을 경우 인증을 취소하여야 한다.

라. 우리나라의 인증제도

1) 개인정보 보호 인증(PIMS), 정보보호 인증(ISMS), 정보보호 및 개인정보 보호 관리체계 인증(ISMS-P)

우리 법제에서는 개인정보 보호와 관련한 것으로 두 가지 인증제도가 시행되어왔다. 하나는 개인정보 보호법에서 규정하고 있는 개인정보 보호 인증(PIMS, 제32조의 2, 시행령 제34조의2 ~ 제34조의8)이다. 이것은 개인정보 보호위원회가 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 개인정보 보호법에 부합하는지 등에 관하여 인증하는 것이다. 인증심사기준은 고시에 정해진 바와 같고, 심사수행기관이 신청인과 협의를 통해 인증기준 내에서 인증범위, 업무 특성 등을 고려하여 인증심사 항목을 조정할 수 있다.

다른 하나는 정보통신망법에서 규정하고 있는 정보보호 인증(ISMS, 제47조, 시행령 제47조 ~ 제54조, 시행규칙 제3조)이다. 이는 과학기술정보통신부장관이 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 “정보보호 관리체계”라 한다)를 수립·운영하고 있는 자에 대하여 장관이 정한 기준에 적합한지에 관하여 인증하는 것이다. 인증대상자는 정보통신망법에 상세하게 규정되어 있다[393].

<그림5-6> PIMS 인증의 구성요소

<그림5-7> ISMS 인증의 구성요소

393) 정보통신망법에 의하면 인증의무자는 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서, 1.「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망 서비스를 제공하는 자, 2. 집적정보통신시설 사업자, 3. 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 3개월간의 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자이다(제47조 제2항).

이 두 가지 인증을 통합한 것이 정보보호 및 개인정보 보호 관리체계 인증(ISMS-P)이다.

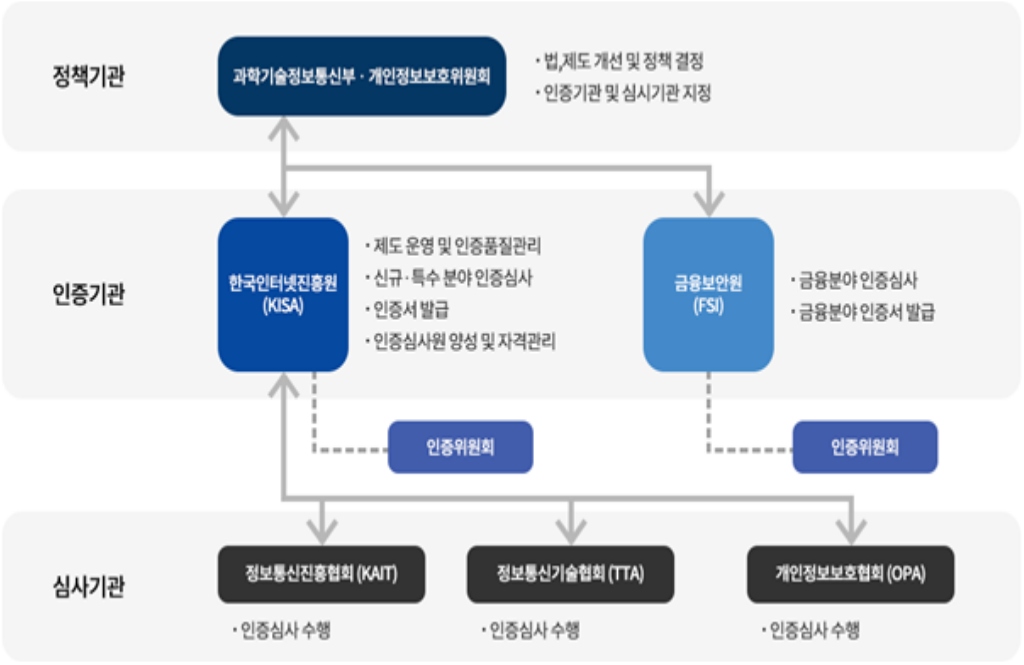
ISMS 인증은 법령상의 의무 인증이다. 즉, 법령에서 특정한 기준에 해당하는 사업자에게 정보보호 및 개인정보 보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인증받을 의무를 부과하고 있다.

<그림5-8> ISMS-P 인증의 구성요소

2) 인증 절차와 관련자

인증체계는 다음과 같이 구성되어 있다. 즉, 법제도 개선 및 정책 결정, 인증기관 및 심사기관 지정 업무를 수행하는 기관은 과학기술정보통신부와 개인정보 보호위원회이다. 인증기관은 한국인터넷진흥원과 금융보안원인데, 정보통신진흥협회, 정보통신기술협회, 개인정보보호협회가 심사기관으로 역할을 한다.

<그림5-9> 인증체계 구성



*출처 : 개인정보보호포털

<그림5-10> 인증심사 절차

*출처 : 개인정보보호협회

3) 인증기관 및 심사기관의 공정성과 독립성

고시는 인증기관 및 심사기관은 인증심사의 공정성 및 독립성 확보를 위해 발생되지 않도록 노력하여야 할 4가지 행위를 들고 있다. 그에 의하면 정보보호 및 개인정보보호 관리체계 구축과 관련된 컨설팅 업무를 수행하는 행위, 정당한 사유 없이 인증절차, 인증기준 등의 일부를 생략하는 행위, 조직의 이익 등을 위해 인증심사 결과에 영향을 주는 행위, 그 밖에 인증심사의 공정성 및 독립성을 훼손할 수 있는 행위가 해당한다.

마. 현재의 인증 등에 대한 평가와 법제 개선방안

1) 법률상 의무인 인증제도 외의 인증

현재 우리 법제상 ISMS 인증은 특정한 요건에 해당하는 기업에게 법률상 인증을 받도록 인증제도가 운용되고 있다. 반면, PIMS는 자발적인 참여에 바탕을 둔 인증제도이다.

2) 독립적이고 전문적인 모니터링 기관이 필요함

우리나라에는 인증과 관련하여 독립적이고 전문적인 모니터링 수행기관이 없다. 그런데, 인증제도가 신뢰받기 위해서는 인증에 대한 모니터링을 수행할 기관이 신뢰할 수 있어야 하고, 독립적이고 전문적인 능력을 갖춘 곳이어야 한다. 그런 점에서 현재의 구조는 심사기관의 독립성을 신뢰하기 어려운 구조이다. 예를 들어 한국정보통신진흥협회는 정보통신서비스 제공자 및 정보통신망과 관련된 사업을 경영하는 자로 구성된 협회이다[394]. 따라서 한국정보통신진흥협회로부터 독립성이 보장되는 전문적 능력을 갖춘 곳에서 모니터링을 수행해야만 신뢰받을 수 있을 것이다. 개인정보보호협회도 통신사들이나 온라인쇼핑몰 등의 사업자들로 구성된 협회로서 모니터링의 독립성을 인정받기 어려운 조직이다. 따라서 이들과 같은 조직이 아니라, 독립적이고 전문적인 모니터링 기관을 통한 모니터링이 이루어질 수 있도록 제도를 개선하는 것이 바람직할 것이다.

394) 방송통신발전기본법 제15조

제6장 범죄예방과 수사 등 분야에서 개인정보 보호

제1절 GDPR의 적용 예외로서 '범죄수사 등'

1. 경찰 디렉티브의 제정취지

GDPR은 "범죄의 예방, 수사, 적발 또는 기소, 형사제재의 집행 그리고 공공의 안전에 대한 위협의 방지 및 그 위협으로부터 공공의 안전의 보호를 목적[395]으로 관할기관(competent authorities)에 의해 이루어지는 개인정보의 처리"에는 적용되지 않는다(GDPR 제2조(2)(d)). 대신에, 유럽연합은 GDPR 제정과 같은 날 '범죄수사 등'의 영역에서 개인정보 보호를 위하여 회원국들이 적용해야 할 지침으로 DIRECTIVE (EU) 2016/680[396]를 제정하였다.[397] GDPR과는 달리 디렉티브는 법적 강제력은 없지만, 유럽연합 회원국은 범죄수사 등의 영역에 적용되는 국내입법에서 디렉티브에 규정된 내용을 반영해야 한다.

디렉티브는 법적 강제력은 없는 대신에, 각 회원국들이 범죄수사 등의 목적으로 개인정보를 처리할 때 준수해야 할 최저기준을 규정한 것이다. 각 국가의 국내법이 범죄수사 등의 영역에서 정보주체의 권리와 자유를 보호하기 위하여 디렉티브가 규정한 사항보다 높은 수준의 보호조치를 규정하는 것은 당연히 허용된다.

---

395) 이하에서 이처럼 GDPR이 적용되지 않는 범죄의 예방, 수사 등의 목적을 통칭할 때에는 '범죄수사 등'이라고 표현할 것이다. 거기에 언급된 여러 가지 목적 중에 어떤 목적을 특별히 명시해야 하는 경우는 별도로 표기한다.

396) DIRECTIVE (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

397) 이하에서 이 디렉티브를 언급할 때에는 단순히 디렉티브라 한다.

2. 경찰 디렉티브의 적용대상

여기에서 디렉티브의 적용대상이 되는 '관할기관(competent authorities)'이란 범죄의 예방, 수사, 적발 또는 기소, 형사제재의 집행 그리고 공공의 안전에 대한 위협의 방지 및 그 위협으로부터 공공의 안전의 보호에 권한이 있는 모든 공공기관(public authority) 뿐만 아니라, 그러한 목적을 위해 공적 권한을 행사할 수 있도록 회원국 법이 권한을 부여한 그 밖의 기구나 기관(any other body or entity)을 포함한다(디렉티브 제3조(7)).

디렉티브의 주된 적용대상은 경찰일 것이다. 범죄의 예방이나 수사를 위한 경찰의 활동은 어떤 사건이 형사범죄인지 여부가 아직 불확실한 단계에서 관련 개인정보를 수집하는 경우도 포함한다. 여기에는 형사소송법이나 경찰 직무에 관한 법령에 규정된 바에 따라 강제조치 권한을 행사하는 것도 당연히 포함된다. 그리고 수사 외에 범죄의 예방이라든가 공공의 안전에 대한 위협에 대응하기 위한 경찰활동도 포함된다.

회원국의 법체계에서 경찰 등 법집행기관에 범죄수사 등의 목적에 필수적이지 않은 다른 업무권한을 부여한 결과 그와 같은 업무의 수행을 위하여 개인정보를 처리하는 경우가 있을 수 있는데, 이때에는 GDPR의 적용을 받는다.

그리고 여기에서 '범죄(criminal offence)'는 유럽연합 법의 독자적인 개념으로 유럽사법재판소의 해석에 따른다.

제2절 GDPR과의 차이점 분석

1. 개인정보 처리원칙

가. 투명성 원칙의 적용 제한(디렉티브 제4조)

GDPR 제5조(1)(a)는 개인정보 처리의 원칙으로 적법성, 공정성과 투명성을 규정하고 있는 반면에, 디렉티브 제4조(1)(a)는 적법성과 공정성을 규정하면서 투명성 원칙은 명시적으로 규정하지 않는다. 범죄수사 등을 위해서는 비밀수사라든가 비디오감시와 같이 비밀리에 개인정보를 수집하는 활동이 허용될 수 있어야 한다는 이유에서이다. 물론 그처럼 비밀리에 수행되는 개인정보 수집활동도 적법성의 원칙에 따라 명확한 법적 근거를

갖추어야 하고, 필요최소한도의 수집에 그쳐야 한다.

또한 최소처리원칙(data minimisation)과 관련하여, GDPR 제5조(1)(c)는 개인정보의 처리목적에 비추어 “필요한 것에 한정(limited to what is necessary)”되어야 한다고 규정하는 반면에, 디렉티브 제4조(1)(c)는 개인정보의 처리목적에 비추어 “과도하지 않아야(not excessive)” 한다고 규정하고 있어, 미묘한 차이가 있다.

나. 정보의 삭제 또는 보관의 기한 제한(디렉티브 제5조)

GDPR은 개인정보를 식별 가능한 형태로 보관하는 것은 개인정보의 처리목적에 필요한 기간을 넘어서는 안 된다고 규정하고 있으며(제5조(1)(f)), 이에 상응하여 정보주체가 컨트롤러에게 자신에 관한 개인정보를 부당한 지체 없이(without undue delay) 삭제하도록 요청할 권리를 보장하고 있다(제17조). 컨트롤러는 개인정보가 처리목적에 비추어 더 이상 필요하지 않은 경우 또는 정보주체가 개인정보 처리의 근거가 되었던 동의를 철회하고 달리 개인정보 처리의 법적 근거가 없는 경우 등 GDPR 제17조(1)(a)~(f)의 요건에 해당하면 컨트롤러는 삭제의무를 진다(제17조).

반면에, 개인정보의 삭제에 관하여 디렉티브 제5조에 의하면, 범죄수사 등 디렉티브의 적용영역에서 처리되는 개인정보에 대해서 각 회원국은 개인정보를 삭제하거나 또는 계속 보관의 필요성을 주기적으로 심사하기 위한 적절한 기한을 설정해야 하며 그러한 기한의 준수를 보장하는 절차적 수단을 마련해야 할 의무를 진다.

디렉티브의 적용영역에서 정보주체의 삭제요청권과 컨트롤러의 삭제의무는 GDPR보다 제한적이다. 개인정보의 처리가 디렉티브 제4, 8, 10조에 따른 회원국의 법규정을 침해하거나, 컨트롤러의 법적 의무를 이행하기 위하여 개인정보가 삭제되어야 하는 경우에 한하여 정보주체의 삭제권(그리고 컨트롤러의 삭제의무)이 인정된다(디렉티브 제16조(2)).

다. 범죄와 관련하여 정보주체의 범주의 구별(디렉티브 제6조)

범죄의 예방이나 수사, 기소, 형집행 등의 영역에서는 피의자나 피해자 등 정보주체의 범주를 분명하게 구별하여 개인정보를 처리하는 것이 매우 중요하다. 이에 따라 디렉티브의 적용영역에서 회원국은 컨트롤러에게 가능한 한 정보주체의 범주를 명확하게 구별

하여 개인정보를 처리하도록 해야 한다(제6조). 범죄와 관련하여 정보주체의 범주는 아래와 같이 구별되어야 한다 :

(a) 범죄를 저질렀거나 저지르려 한다고 믿을 만한 상당한 이유가 있는 사람,

(b) 유죄판결이 확정된 사람,

(c) 범죄피해자 또는 일정한 사실로 볼 때 범죄피해자라고 믿을 만한 근거가 있다고 인정되는 사람,

(d) 그 밖의 사람들, 예를 들어, 수사절차나 이후의 형사절차에서 진술을 위하여 소환될 가능성이 있는 사람, 범죄에 관한 정보를 제공할 수 있는 사람, (a)와 (b)에 해당하는 사람의 지인이나 동료 등.

이러한 정보주체의 범주의 구별은 무죄추정의 권리를 적용하는데 장애가 되어서는 안 된다(전문 31).

라. 정보의 정확성 ; 사실에 근거한 개인정보와 평가적 의견에 기초한 개인정보의 구별 (디렉티브 제7조)

개인정보처리 원칙의 하나인 정확성 원칙은 처리되는 개인정보가 정확해야 하며 처리 목적상 필요하다면 최신의 것으로 유지되어야 한다는 원칙을 말한다(GDPR 제5조(1)(d)). 정확성 원칙은 범죄수사 목적의 개인정보 처리에도 당연히 적용되어야 한다. 다만, 형사절차에서는 개인정보를 포함하는 진술들은 대개 진술자의 주관적인 인식에 기초한 것이라는 점에서 객관적인 사실증명이 항상 가능한 것은 아니라는 특수성을 고려해야 한다. 따라서, 예를 들어, 형사절차에서 행해진 진술에 대하여 정확성 원칙은 진술내용(에 포함된 개인정보)의 정확성을 말하는 것이 아니라, 특정한 진술이 행해졌다는 사실의 정확성을 담보하면 된다.

이러한 의미에서 디렉티브는 사실에 근거한 개인정보와 평가적 의견에 기초한 개인정보를 명확하게 구별할 것을 요구한다(제7조(1)).

마. 개인정보 처리의 적법성(디렉티브 제8조)

디렉티브 제8조(1)에 따르면, 회원국은 유럽연합 법이나 회원국 법에 근거가 있고, 범죄수사 등 디렉티브 제1조(1)에 규정된 목적을 위하여 관할기관이 수행하는 직무집행에 필요한 범위에 한해서만 개인정보의 처리가 적법하도록 규정해야 한다. 그리고 디렉티브의 범위에 속하는 개인정보의 처리에 관한 회원국 법은 최소한 개인정보 처리의 목적과 처리되는 개인정보의 범위를 구체적으로 규정해야 한다(제8조(2)).

일반적으로 정보주체의 동의는 개인정보 처리의 적법성의 근거가 된다(GDPR 제6조). 그런데, 경찰·검찰 등 법집행기관은 범죄의 예방·수사·기소 등의 직무를 수행하는데 필요한 개인정보를 제공하도록 개인에게 요구하거나 명령할 권한을 가진다. 그러한 경우에 정보주체의 동의는 개인정보 처리의 법적 근거가 될 수 없다. 정보주체가 경찰 등 법집행기관의 요구에 따라 개인정보를 제공해야 할 법적 의무를 지는 경우라면 개인의 자유롭고 진지한 의사에 따른 동의를 인정할 수 없기 때문이다(전문 35).

한편, 디렉티브는 수사목적의 DNA 시료채취라든가 형사제재의 집행을 위한 위치추적장치 부착 등의 경우처럼 디렉티브의 목적을 위한 개인정보 처리가 정보주체의 동의에 의하여도 가능하도록 법에 관련 규정을 둘 수 있다고 한다(전문 35).

바. 특수 범주의 개인정보의 처리(디렉티브 제10조)

인종, 민족, 정치적 견해, 종교적·철학적 신념, 노동조합 멤버쉽을 알 수 있게 해주는 개인정보의 처리, 유전자정보, 자연인을 고유하게 식별할 목적의 생체정보, 건강관련 정보, 자연인의 성생활이나 성적 지향에 관한 정보(이하 '민감정보'라 함)에 관하여 GDPR 제9조는 그러한 민감정보의 처리를 원칙적으로 금지하면서 예외적으로 민감정보의 처리가 허용되는 일정한 요건을 열거하고 있다.

이에 비하여, 디렉티브 제10조는 범죄수사 목적의 민감정보 처리에 관하여 GDPR보다 비교적 완화된 요건 하에 폭넓게 용인하는 태도를 취한다. (a) 유럽연합 법이나 회원국 법이 허용하는 경우; (b) 정보주체나 타인의 생명을 보호하기 위한 경우; 또는 (c) 개인정보의 처리가 정보주체가 명백하게 공개한 개인정보와 관련된 경우로서, '엄격하게 필요한 경우에 한해서(only where strictly necessary)' 그리고 정보주체의 권리와 자유에 대

한 적절한 보호조치가 보장되어야 한다는 조건에서 회원국은 범죄수사의 목적을 위한 민감정보의 처리를 허용할 수 있다.

이러한 요건 중에서 (b)와 (c)는 GDPR 제9조에서도 민감정보를 처리할 수 있는 예외사유로 규정되어 있지만, (a)요건에서 보듯이 디렉티브 제10조는 회원국이 범죄수사의 목적을 위하여 민감정보의 처리를 명시적으로 허용하는 법규정을 두기만 하면 경찰 등 관할기관은 민감정보를 처리할 수 있다. 물론 필요한 최소한도의 처리에 한정되어야 함은 당연하다.

민감정보의 처리에 대하여 정보주체의 명시적인 동의가 있는 경우에는 민감정보의 처리가 가능하도록 법규정을 두어야 하지만, 정보주체의 동의 그 자체만으로는 범죄수사 목적의 민감정보의 처리가 정당화될 수 없다(전문 37). 정보주체의 권리와 자유에 대한 적절한 보호조치로는 가령 민감정보를 대상자의 다른 개인정보와 연결해서만 수집할 수 있도록 한다든가, 정보처리의 안전성 보장, 관할기관 직원들의 정보접근에 대한 엄격한 통제, 민감정보 이전의 금지 등을 들 수 있다(전문 37).

사. 자동화된 개별 의사결정(디렉티브 제11조)

디렉티브 제11조(1)은 정보주체에게 불리한 법적 효력 또는 중대한 효과를 미치는 의사결정이 프로파일링 등 오로지 자동화된 처리에만 근거해서 이루어지는 것을 원칙적으로 금지하도록 규정한다. 다만, 컨트롤러에게 적용되는 유럽연합 법이나 회원국 법이 정보주체의 권리와 자유 - 최소한 컨트롤러 측에서 인간의 개입을 보장받을 권리 - 를 보장하기 위한 적절한 보호조치를 제공하면서 이를 허용하는 경우는 예외로 한다.

그리고 제1항에서 말하는 자동화된 의사결정은 정보주체의 권리와 자유 및 정당한 이익을 보호하기 위한 적절한 조치가 제공되는 경우가 아니라면 디렉티브 제10조에 규정된 특수 범주의 개인정보(민감정보)에 근거해서는 안 된다(제11조(2)).

위와 같은 디렉티브 제11조(1)과 (2)의 내용을 자동화된 의사결정의 적용을 받지 않을 권리를 정보주체의 권리로 규정하고 있는 GDPR 제22조와 비교해 보면, 몇 가지 차이가 발견된다. 첫째, 디렉티브 제11조에서 원칙적으로 금지되는 자동화된 의사결정은 '불리한(adverse)' 법적 효력 또는 중대한 효과를 미치는 경우에 한정된다. GDPR 제22조에는

‘불리한’이라는 문구가 없다. 둘째, 자동화된 의사결정이 허용되는 예외사유는 유럽연합 법이나 회원국 법에 법적 근거가 있을 것과 유럽연합 법이나 회원국 법이 정보주체의 권리와 자유를 위한 적절한 보호조치[398]를 제공할 것을 요건으로 하는데, 이는 GDPR 제22조(2)(b)와 유사하긴 하나 ‘정보주체의 정당한 이익’을 위한 보호조치는 제외되어 있다는 점에서 다소 완화되어 있다. 셋째, 민감정보에 근거한 자동화된 의사결정에 대해서도 디렉티브는 GDPR 제22조(4)보다 완화된 요건 하에 폭넓게 허용하는 태도를 취하고 있다.

한편, 프로파일링이 디렉티브 제10조에 규정된 민감정보를 근거로 하여 개인에 대한 차별의 결과를 낳는다면 이는 유럽연합 법[399]에 따라 금지되어야 한다(제11조(3)). 이는 범죄수사 등의 목적으로 민감정보에 근거하여 이루어지는 개인에 대한 프로파일링이 차별의 결과로 이어지면 안 된다는 점을 특별히 규정한 것이다.

2. 정보주체의 권리 보장 관련

가. 정보주체의 권리행사를 위한 통지(디렉티브 제12조)

디렉티브 제12조는 컨트롤러의 개인정보 수집시의 정보제공, 그리고 정보주체의 열람권 등의 권리행사와 관련하여 행해지는 각종 통지·고지를 간결하고 이해하기 쉽고 접근하기 쉬운 방식으로 제공하도록 할 것을 규정하고 있다. 이는 정보주체의 권리행사를 가능하게 하는 조치로, GDPR 제12조에 상응하는 규정이다. 다만, 범죄수사 등 목적의 개인정보 처리에 적용되는 디렉티브는 GDPR보다 투명성 원칙을 제한적으로 적용하는 경향을 보이고 있는바, 이에 따라 디렉티브 제12조(1)에서는 “투명한 방식의 제공”이라는 문구가 제외되어 있다.

그리고 정보주체가 그 권리에 입각해서 컨트롤러에게 일정한 요청을 하는 경우에 GDPR은 ‘부당한 지체 없이, 요청을 접수한 후 1개월 이내에’[400] 그 요청에 따라 취해

398) 그러한 보호조치로는, GDPR 제22조(3)의 경우와 유사하게, 정보주체에 대한 통지, 인간의 개입을 보장받을 권리, 자신의 견해를 표명할 권리, 의사결정에 관한 설명을 획득할 권리, 결정에 불복할 권리 등을 말한다(전문 38).
399) 이는 유럽연합 기본권헌장 제21조와 제52조에 규정된 요건이 적용된다는 의미이다(전문 38).
400) 필요하다면 추가로 2개월이 연장될 수 있다(GDPR 제12조(3)).

진 조치에 관한 정보를 정보주체에게 제공하도록 규정하고 있는 반면에, 디렉티브는 '요청을 접수한 후 1개월 이내'라는 엄격한 제한을 두지 않는다는 점에서 차이가 있다(디렉티브 제12조(3)).

또한 GDPR 제12조(4)는 컨트롤러가 정보주체의 요청에 대응한 조치를 취하지 않은 경우에 그 이유와 불복할 권리에 대해 정보주체에게 고지해야 할 의무를 규정하고 있는데, 디렉티브에는 이에 상응한 컨트롤러의 고지의무에 관한 일반 규정이 존재하지 않는다. 아래에서 서술하는 바와 같이, 디렉티브 제13~16조가 정보주체의 권리에 대한 제한조치를 허용하고 있음을 감안하여 디렉티브는 GDPR 제12조(4)과 같은 일반적인 고지의무를 규정하지 않는 대신에, 개별적인 경우에 불복할 권리에 관한 고지의무를 별도로 규정하는 방식을 채택하고 있다[401].

나. 컨트롤러의 개인정보 수집시 정보제공(디렉티브 제13조)

GDPR은 컨트롤러가 개인정보를 수집할 때 정보주체에게 일정한 정보(information)를 제공해야 할 의무가 있음을 규정하면서, 이때 제공되어야 할 정보의 범위와 제공 시기에 대해 상세하게 규정하고 있다. 제13조는 컨트롤러가 정보주체로부터 개인정보를 수집할 때 제공해야 할 사항과 제공 시기에 대해서, 그리고 제14조는 컨트롤러가 정보주체가 아닌 다른 소스로부터 개인정보를 수집한 경우에 대해서 규정한다. 디렉티브에서는 제13조가 GDPR 제13조, 제14조에 상응하는 규정인데, 몇 가지 중요한 차이점이 있다.

첫째, 디렉티브 제13조는 컨트롤러가 개인정보를 수집한 원천이 정보주체 본인인지 아닌지에 따른 구별을 두지 않는다. 아마도 경찰이나 기타 법집행기관들은 범죄의 예방·수사 등 업무의 특성상 정보주체가 아닌 다른 소스로부터 개인정보를 수집하는 경우가 많고 그러한 개인정보의 수집 자체를 정보주체에게 비밀로 유지해야 할 필요가 있을 수 있기 때문이다.

둘째, 디렉티브 제13조 제1항과 제2항은 컨트롤러가 정보주체에게 제공해야 할 정보의 내용과 범위를 열거하고 있는데, GDPR에서 컨트롤러의 제공의무로 규정된 것보다 약간

401) 예를 들어, 디렉티브 제15조 제3항은 컨트롤러가 디렉티브 제15조 제1항에 따라 정보주체의 접근권을 제한한 경우에 컨트롤러가 그 사유를 정보주체에게 부당한 지체 없이 고지할 의무를 지도록 하면서도 이것 또한 일정한 예외가 적용되도록 규정하고 있으며, 이 경우에 불복할 권리를 고지하도록 규정하고 있다.

축소되어 있다. 대신에 디렉티브는 컨트롤러가 필수적으로 제공해야 할 '최소한도'의 사항을 규정한 것이라고 한다.

가장 큰 차이는 개인정보를 제3국이나 국제기구에 이전(transfer)하는 경우이다. GDPR 제13조와 제14조는 개인정보를 제3국이나 국제기구에 이전할 예정이거나 이전한 사실, 집행위원회의 적정성 결정의 유무, 그리고 이용 가능한 보호조치에 대한 안내정보를 제공하도록 규정하고 있지만, 디렉티브는 제3국이나 국제기구에 개인정보를 제공한 경우에도 단지 개인정보의 수령인(recipients)이나 수령인의 범주에 관한 정보를 제공하는 것으로 규정하고 있다.

셋째, 디렉티브는 회원국이 아래와 같은 사유를 근거로 하는 경우에 관련 개인의 기본권과 정당한 이익을 적절하게 고려하면서 민주사회에서 필요한 적절한 한도에서 제13조 제2항에 따른 정보의 제공을 연기·제한·생략하는 입법조치를 취할 수 있다고 규정한다(제13조(3)) : (a) 공식적 또는 법적 탐문, 수사나 절차에 대한 장애의 방지, (b) 범죄의 예방, 탐지, 수사, 소추, 또는 형사제재의 집행에 대한 장애의 방지, (c) 공공의 안전의 보호, (d) 국가의 안전의 보호, (e) 다른 사람들의 권리와 자유의 보호.

회원국은 범죄수사 등 목적으로 이루어지는 개인정보 처리 중에서 제3항의 사유에 따라 정보주체에 대한 정보의 제공이 전부 또는 일부 연기·제한·생략될 수 있는 처리 범주를 회원국의 법령으로 정할 수 있다(디렉티브 제13조(4)).

다. 정보주체의 접근권의 보장과 제한(디렉티브 제14, 15조)

디렉티브 제14조에 따라 회원국은 정보주체의 권리로 본인에 관한 개인정보가 처리되고 있는지 여부에 대해 컨트롤러로부터 확인을 받을 권리를 보장해야 하며, 이때 처리되는 개인정보와 처리목적 등 디렉티브 제14조 (a)~(g)에 규정한 정보에 접근할 권리를 보장해야 한다. 접근할 수 있는 정보의 범위에서 미세한 차이가 있기는 하지만, 이처럼 범죄수사 등의 목적으로 이루어지는 개인정보 처리에 대해서도 정보주체의 접근권을 보장해야 한다는 점은 GDPR 제15조와 동일하다.

그런데 GDPR에서 정보주체의 접근 요구가 있는 경우에 처리가 진행 중인 개인정보의 사본을 제공하도록 규정하고 있는 것과는 다르게, 디렉티브에는 그러한 규정이 없다. 디

렉티브 전문에 의하면, 정보주체가 디렉티브에 의하여 부여되는 권리를 행사할 수 있도록 처리가 진행 중인 개인정보에 대한 '전체 요약(full summary)'을 제공해도 충분하다고 한다(전문 43)[402].

무엇보다 큰 차이는 접근권에 대한 제한조치가 넓게 허용된다는 점이다. 디렉티브 제15조는 회원국의 법체계에서 관할기관이 범죄수사 등의 목적으로 개인정보를 처리하는 경우에 정보주체의 접근권을 제한할 수 있도록 허용한다. 이에 의하면, 회원국은 아래와 같은 사유를 근거로 하는 경우에 '관련 개인의 기본권과 정당한 이익을 적절하게 고려하면서 민주사회에서 필요한 적절한 한도에서' 정보주체의 접근권의 전부 또는 일부를 제한하는 입법조치를 취할 수 있다(제15조(1)) : (a) 공식적 또는 법적 탐문, 수사나 절차에 대한 장애의 방지, (b) 범죄의 예방, 탐지, 수사, 소추, 또는 형사제재의 집행에 대한 장애의 방지, (c) 공공의 안전의 보호, (d) 국가의 안전의 보호, (e) 다른 사람들의 권리와 자유의 보호. 이때 회원국은 위와 같은 사유를 근거로 해서 정보주체의 접근권이 전부 또는 일부 제한되는 처리 범주를 회원국의 법령으로 정할 수 있다(제15조(2)).

접근권의 제한은 일률적 또는 포괄적으로 행해져서는 안 된다. 컨트롤러는 각 개별 사례마다 구체적이고 개별적인 심사를 통해 위와 같은 사유를 근거로 접근권에 대한 제한이 필요한지 여부를 심사해야 한다(전문 44).

이렇게 정보주체의 접근권이 제한되는 경우에, 회원국은 컨트롤러로 하여금 접근권이 거부 또는 제한되었다는 점과 그 사유를 부당한 지체 없이 정보주체에게 서면으로 알려주도록 규정해야 한다. 다만, 그러한 정보의 제공이 제15조 제1항 (a)~(e)에 규정된 목적을 위태롭게 하는 경우에는 생략할 수 있다. 한편, 회원국은 컨트롤러가 정보주체에게 감독기관에 민원을 제기하거나 사법적 구제절차를 취할 수 있다는 점을 알려주도록 규정을 두어야 한다(디렉티브 제15조(3)). 컨트롤러는 위와 같은 결정의 사실적·법적 근거에 관한 기록을 보존해야 하며, 감독기관이 이를 이용할 수 있도록 해야 한다(디렉티브 제15조(4)).

402) 물론 처리 중인 개인정보의 사본을 제공하는 것은 당연히 가능하다.

라. 정정・삭제・처리제한권의 보장과 제한(디렉티브 제16조)

GDPR이 정보주체의 권리로 규정한 정정권(GDPR 제16조), 삭제권(제17조), 처리제한권(제18조)은 원칙적으로 범죄수사 등 목적의 개인정보 처리에서도 적용되어야 한다(디렉티브 제16조). 다만, 범죄수사 등의 목적으로 관할기관이 개인정보를 처리하는 경우에는 정보주체의 동의에 의한 수집은 원칙적으로 의미가 없으며 투명성 원칙의 적용이 제한적일 수밖에 없다는 점에서, 디렉티브에서 규정한 삭제권과 처리제한권의 근거사유에 관한 규정은 GDPR과는 다소 차이가 있다(디렉티브 제16조(2),(3)). 특히 개인정보의 삭제권은 사실상 회원국의 법령이 디렉티브에 따라 개인정보 처리의 합법성의 기준으로 규정한 것을 위반한 경우 또는 개인정보를 삭제할 의무를 부과하고 있는 경우에만 인정된다는 점에서 GDPR이 규정한 삭제권보다 훨씬 제한적이다. 또한 디렉티브는 정보의 정확성에 대한 이의가 제기되었고 그 정확성 여부가 확정되지 않은 경우와 증거사용을 목적으로 개인정보를 보존할 필요가 있는 경우에는 컨트롤러로 하여금 삭제 대신에 처리제한을 하도록 규정한다(제16조(3)(b)). 개인정보의 정확성에 대한 이의가 제기됨으로써 처리제한이 이루어진 경우에는 컨트롤러는 처리제한을 해제하기 전에 정보주체에게 통지해야 한다(제16조(3)).

컨트롤러가 위와 같은 정정・삭제・처리제한의 요청을 거절한 경우에는 거절한다는 점과 그 사유를 서면으로 정보주체에게 통지해야 한다. 그러나 디렉티브에 의하면, 회원국은 아래와 같은 사유를 근거로 하는 경우에 '관련 개인의 기본권과 정당한 이익을 적절하게 고려하면서 민주사회에서 필요한 적절한 한도에서' 컨트롤러의 통지의무의 전부 또는 일부를 제한하는 입법조치를 취할 수 있다 : (a) 공식적 또는 법적 탐문, 수사나 절차에 대한 장애의 방지, (b) 범죄의 예방, 탐지, 수사, 소추, 또는 형사제재의 집행에 대한 장애의 방지, (c) 공공의 안전의 보호, (d) 국가의 안전의 보호, (e) 다른 사람들의 권리와 자유의 보호(제16조(4)). 이때 회원국은 컨트롤러가 정보주체에게 감독기관에 민원을 제기하거나 사법적 구제절차를 강구할 수 있다는 점을 알려주도록 해야 한다(제16조(4)).

그 밖에 디렉티브 제16조는 컨트롤러가 부정확한 개인정보를 정정한 경우에 그 부정확한 개인정보를 제공한 관할기관에 통지하도록 할 것, 그리고 제16조 제1, 2, 3항에 따

라 개인정보의 정정・삭제・처리제한이 이루어진 경우에 컨트롤러로 하여금 이를 수령인에게 통지하고 수령인이 자신의 책임 하에 개인정보의 정정・삭제・처리제한을 하도록 규정할 것을 주문하고 있다(제16조(5), (6)).

마. 감독기관을 통한 권리 행사(디렉티브 제17조)

회원국은 하나 이상의 감독기관을 두고 경찰 디렉티브의 준수를 자문 및 감독하여야 하며, 감독기관들은 국내외적으로 다른 감독기관들과 상호 협력 및 지원할 수 있어야 한다. GDPR에 따라 회원국에 이미 설립된 감독기관이 있다면 이 디렉티브에 따라 설립될 감독기관이 수행해야 할 업무에 대해 소관하도록 맡길 수 있다(전문 76; 제41조제3항). 즉, 경찰 디렉티브 목적으로 설립된 감독기관은 GDPR 상의 감독기관과 같을 수도 있지만 회원국의 헌법상, 조직법상, 행정상 체계에 따라 독립성의 기준에 부합하는 다른 감독기관을 선택할 수 있다(FRA, 2018: 290; 전문 77). 대부분의 국가는 GDPR과 경찰 디렉티브 모두를 소관하는 하나의 감독기관을 두고 있지만 몇몇 국가는 경찰 디렉티브의 소관 범위에 대해 감독기관의 권한을 제한하고 있다[403]. 벨기에의 경우 GDPR과 경찰 디렉티브를 소관하는 감독기관을 분리하여 각각 두고 있다[404].

경찰 디렉티브는 개인정보 보호 감독기관에 대하여 제6장(독립적 감독기관)에서 제41조(감독기관), 제42조(독립성), 제43조(감독기관 구성원에 대한 일반 조건), 제44조(감독기관 설립에 관한 규칙), 제45조(주무 권한), 제46조(업무), 제47조(권한), 제48조(침해 보고), 제49조(활동 보고서)를 규정하였으며 제7장(협력)에서 제50조(상호 지원), 제51조(보호위원회 업무)를 두었다.

경찰 디렉티브의 감독기관은 GDPR과 그 독립성, 구성, 설립, 주무 권한에 대한 규정이 대체로 유사하다. 감독기관의 업무에 있어서도 GDPR과 마찬가지로 정보주체의 진정을

403) INFORM(2018), “D2.5 Review report on Directive (EU) 2016/680 aimed at the legal practitioners”. Ref. Ares(2018)3815178, p41. <http://informproject.eu/wp-content/uploads/2018/05/D2.5.pdf>.

404) Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 2019.4.12., "European Data Protection Supervisor 2019. Data Protection Law Enforcement Directive(EU) 2016/680 transposition Updated State of play in the Member States", <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=14010>.

접수하고 심리할 수 있는 권한을 부여하였고, 진정 절차 및 진정 결과에 대한 정보를 제공하도록 하였다. 디렉티브에 규정된 권리 행사가 거부된 정보주체는 소관 감독기관 또는 법원에 이의를 제기할 수 있다. 감독기관은 디렉티브 침해 행위를 사법부에 고발하거나 소송을 개시하는 등 관여할 권한 또한 부여받았다[405].

그러나 경찰 디렉티브 감독기관의 업무는 GDPR 감독기관의 업무와 몇 가지 점에서 차이가 있다. 우선 법집행 업무의 특수성으로 인해 민간 업무에 적용되는 표준 계약 조항, 행위지침, 인증제도, 제3국이나 국제기구 개인정보 이전 시 보호조치로서 계약 조항 및 기업 규칙 부분이 규정되어 있지 않다. 또한 GDPR에서 상당한 비중을 할애하여 규정하고 있는 주감독기관 등 유럽연합 전체의 일관성 메커니즘이 모두 생략되어 있는데 이는 각국 법집행 업무의 특수성 및 보안을 고려한 것으로 보인다. GDPR에서 감독기관의 업무로 규정하고 있는 개인정보 보호 영향평가 관련 목록 작성 및 공표에 대한 규정[406], 제3국이나 국제기구 개인정보 이전 시 보호조치로서 공공기관 간 약정에 대한 감독 규정[407], 감독기관의 시정 조치와 관련한 내부 기록 보관 규정[408]은 경찰 디렉티브에 생략되어 있다.

경찰 디렉티브 감독기관의 권한은 전반적으로 GDPR에 비하여 축소하여 규정되었다. 우선 조사권과 관련하여서 감독기관의 자료 접근권(power to obtain access)만을 남기고 자료제출 명령권(power to order)[409]을 규정하지 않았으며, 개인정보 보호 감사의 형태로 조사를 수행할 권한[410], 컨트롤러나 프로세서에게 규정 위반 혐의를 통지할 권한[411], 정보 처리 장비 및 수단에 대한 접근권을 포함하는 부지 접근권[412] 등이 삭제되어 있다. 또 시정조치와 관련해서 컨트롤러나 프로세서에게 견책 처분을 내릴 권한[413], 정보주체의 권리행사 요청에 응할 것을 명령할 권한[414], 개인정보 침해사실을 정보 주체에게 알

405) INFORM(2018), op. cit., p40.
<http://informproject.eu/wp-content/uploads/2018/05/D2.5.pdf>.
406) GDRP 제57조 제1항 (k)호
407) GDRP 제57조 제1항 (r)호
408) GDRP 제57조 제1항 (u)호
409) GDPR 제58조 제1항 (a)호
410) GDPR 제58조 제1항 (b)호
411) GDPR 제58조 제1항 (d)호
412) GDPR 제58조 제1항 (f)호
413) GDPR 제58조 제2항 (b)호
414) GDPR 제58조 제2항 (c)호

리도록 명령할 권한[415], 개인정보 정정 또는 삭제나 처리 제한을 명령하고 개인정보를 공개받은 수령자에 대한 조치 통지를 명령할 권한[416], 제3국이나 국제기구의 수령자에 대한 정보 흐름 중단을 명령할 권한[417] 등이 규정되어 있지 않다. 자문권과 관련하여서는 공익을 위한 컨트롤러 업무 수행에 대한 사전 허가 권한[418]이 삭제되었다.

경찰 디렉티브는 외부적인 감독을 제한하는 한편으로 소관 기관 내부적으로 디렉티브 침해에 대한 기밀 보고를 장려하기 위한 체계를 갖추도록 규정하였다(디렉티브 제48조).

제3절 우리나라의 수사 영역에서 개인정보 보호와 통제에 관한 규율과 제도적 개선방안

유럽연합 경찰 디렉티브는 GDPR에 비해 일부 규정이 완화되어 있지만 경찰 등 법집행 기관에 대해서도 원칙적으로 개인정보 보호 원칙 및 독립적인 감독을 적용하도록 하였다. 이러한 유럽의 규범과 비교하여 보았을 때 우리나라 현행 개인정보 보호법은 범죄수사 및 형집행과 관련한 개인정보 처리에 대해서 많은 예외 규정을 두고 있으며, 이에 수반하는 감독 또한 미흡하게 이루어지고 있다.

첫째, 현행 개인정보 보호법은 공공기관이 보유한 개인정보에 대하여 수사기관이 범죄수사를 위해서 필요로 하는 경우 특별한 요건이나 절차 없이도 목적 외로 제공하도록 하였다. 원칙적으로 개인정보처리자는 개인정보를 적법한 수집목적에 따른 범위를 초과하여 이용하거나 제3자에게 제공하여서는 아니 된다(개인정보 보호법 제18조 제1항). 그럼에도 개인정보처리자가 보유하고 있는 개인정보를 수집·이용 목적 이외의 용도로 제공하기 위해서는 정보주체의 별도 동의나 다른 법률의 특별한 규정을 요구하는 등 개인정보 보호법에서 열거하는 예외에 해당해야 한다(동법 제18조 제2항). 그런데 이 조항은 공공기관이 보유한 개인정보에 대하여 목적 외 이용·제공의 광범위한 예외를 인정하고 있다. 특히 범죄수사 편의를 위해 공공기관이 보유하고 있는 개인정보에 대해서 정보주체의 동의 없이 목적 외로 이용 또는 제공할 수 있게 하기 위한 목적으로[419], "범죄의

415) GDPR 제58조 제2항 (e)호
416) GDPR 제58조 제2항 (g)호
417) GDPR 제58조 제2항 (j)호
418) GDPR 제58조 제3항 (c)호

수사와 공소의 제기 및 유지를 위하여 필요한 경우” 공공기관이 보유한 개인정보에 대해서 특별한 제한 없이 목적 외로 제공하도록 하였다(동조동항 제7호). 공공기관이 보유하고 있는 개인정보의 목적 외 제공에 대한 이러한 예외는 구금시설이 형(刑) 및 감호, 보호처분의 집행을 위하여 필요로 하는 경우(동항 제9호)에도 동일하게 적용된다. 이하에서는 이 예외 조항이 수사기관 뿐 아니라 구금시설에도 해당하는 경우 ‘범죄수사 등’으로 서술한다.

이러한 폭넓은 예외 규정은 동일한 범죄수사의 목적이라 하더라도 신용정보법(제32조 제6항 제5호)이나 「금융실명거래 및 비밀보장에 관한 법률」(제4조 제1항 제1호)에서 데이터전문기관을 포함한 신용정보회사등이 보유한 개인신용정보 또는 금융회사등이 보유한 거래정보 등에 대해서는 법원의 제출명령 또는 법관이 발부한 영장에 따라 제공하도록 규정한 것과 큰 차이를 보인다. 중소기업은행, 한국산업은행, 한국수출입은행, 우체국 등 공공기관에 해당하는 금융기관의 경우, 보유하고 있는 개인정보를 개인정보 보호법에 의해 범죄수사 목적으로 수사기관 등 제3자에게 제공할 때에는 아무런 제한을 두지 않고 다만 금융거래정보에 한하여만 법원이나 법관의 심사를 의무적으로 요구하면서 한층 더 차별적으로 보호하고 있다.

특히 범죄수사 등을 위하여 필요한 경우 공공기관이 제공하는 개인정보에는 특별히 보호해야 할 민감정보가 포함되어 있다. 헌법재판소는 2018년 건강보험 요양급여내역 제공 사건에서 서울용산경찰서장이 파업 중인 전국철도노동조합의 청구인들을 검거하기 위하여 청구인들의 약 2년 또는 3년에 걸친 장기간의 요양급여내역을 제공받은 행위가 불가피하였다고 보기 어려워 위헌이라고 결정하였다(헌재 2018. 8. 30. 결정 2014헌마368). 다만 헌법재판소는 수사기관이 범죄의 수사를 위하여 불가피한 경우 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고 영장주의가 적용되지 않는 임의수사에 의하여 민감정보를 제공받을 수 있다고 보았다. 2019년 국정감사에 따르면 이 결정 이후로도 국민건강보험공단이 수사기관인 경찰, 검찰, 국정원, 법원에 제공하는 개인 의료정보가 계속 증가하고 있다. 공단은 헌재 결정 이후 상병명, 의사소견서, 장기요양등급의 경우 영장에 의해서만 제공하도록 지침과 관행을 개선하였다고 설명하였지만, 영장 통계는 관리하고 있지 않았으며 요양기관번호와 전화번호는 제한 없이 제공하고 있

419) 행정안전부(2016), 개인정보보호법령 및 지침·고시 해설. p105.

어 정보주체의 건강상태에 대한 민감정보 노출에 대한 대책이 없었다.

영상정보처리기기의 설치·운영 제한 역시 범죄의 예방 및 수사를 위하여 필요한 경우 광범위하게 허용되고(법 제25조 제1항 제2호), 공공기관 영상정보처리기기인 경우 다른 목적으로 설치·운영 중이라 하더라도 범죄수사 등에 필요한 경우 위 제18조 제2항에 따라 특별한 요건이나 절차 없이 수집 목적 외로 수사기관등에 제공될 수 있다.

<표6-1> 국민건강보험공단이 수사기관에 제공한 개인 건강정보 현황

구분		헌재결정이후	2018년	2017년
총계		571,473	245,790	398,180
법원	재판업무	4,371	7,121	7,654
	심문서(의견제출) 회신 등	29	48	1
검찰	수사목적	4,145	34,233	45,856
	재산형 집행 등	13	577	5,952
	재판업무	-	18	5
경찰	수사목적	557,292	198,358	336,809
	총포소지 허가 등	3,665	3,784	1,303
국정원	국가안전보장을 위한 정보분석 등	1,958	1,651	600

*출처: 윤소하 국회의원 보도자료(2019. 10. 6.)

공공기관은 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 보호위원회가 고시로 정하는 바에 따라 관보 또는 인터넷 홈페이지 등에 게재하여야 하지만, 위와 같이 법 제18조 제2항 제7호에 의해 공공기관이 수사기관에 제공한 개인정보 처리에 대해서는 제외한다(법 제18조 제4항).

그 뿐 아니라 개인정보 보호법은 위의 법 제18조 제2항의 규정과 연동하여 범죄수사 등을 위하여 필요한 경우 민감정보와 고유식별정보의 처리 제한도 제외하도록 하였다. 민감정보는 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보이기 때문에 정보주체에게 별도의 동의를 받거나 법령에서 처리를 요구하거나 허용하는 경우에 한해 그

처리를 제한하도록 특별히 보호받는다(개인정보 보호법 제23조). 민감정보의 처리에 대해서는 1990년 유엔 가이드라인에서 GDPR에 이르기까지 국제 규범 및 각국 개인정보 보호법에서 대체로 유사하게 보호하고 있다. 그런데 국내 개인정보 보호법은 시행령에 위임하여 민감정보로 정한 유전정보, 범죄경력에 관한 정보, 생체인식정보, 인종이나 민족에 관한 정보의 경우 법 제18조 제2항 제5호부터 제9호까지의 규정에 따라 공공기관이 처리하는 경우 민감정보에서 “제외한다”고 규정하고 있다(동법 시행령 제18조). 수사기관등이 범죄수사 등에 필요로 하는 경우 일부 민감정보가 시행령 규정으로 민감정보가 아닌 것으로 간주되는 것이다. 개인정보 보호법은 개인을 고유하게 구별하기 위하여 부여된 식별정보를 특별히 보호하고 있는데 고유식별정보의 처리 제한 규정(개인정보 보호법 제24조) 역시 마찬가지로 범죄수사 등에 대하여 제외한다. 여기에 해당하는 고유식별정보의 범위는 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 등이다(동법 시행령 제19조). 이러한 제외는 국가가 국민의 기본권을 제한하는 수사나 구금 과정에서 국민의 사생활을 현저히 침해할 우려가 있는 민감정보나 온라인과 오프라인 일상에서 광범위하게 개인을 고유하게 식별하는 데 사용되는 고유식별정보를 처리할 때 최소한의 요건이나 절차 없이 오남용할 수 있다는 우려를 낳게 한다. 특히 이러한 제외를 법률에 근거하지 않고 시행령에서만 규정하고 있다는 점에서 위임입법 일탈의 소지가 있다.

둘째, “범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일”의 경우 공공기관에게 의무인 개인정보파일의 등록 및 공개, 개인정보 처리방침의 수립 및 공개에서 제외하고 있다. 이로 인하여 공개된 개인정보파일에 대해 행사할 수 있는 정보주체의 열람권 및 그에 동반하는 정정·삭제권과 정보주체의 처리정지권 및 고지의 권리도 제한하고 있다.

개인정보 보호법에 따르면 공공기관의 경우 운용하고 있는 개인정보파일에 대하여 ① 개인정보파일의 명칭 ② 개인정보파일의 운영 근거 및 목적 ③ 개인정보파일에 기록되는 개인정보의 항목 ④ 개인정보의 처리방법 ⑤ 개인정보의 보유기간 ⑥ 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자 ⑦ 개인정보파일을 운용하는 공공기관의 명칭 ⑧ 개인정보파일로 보유하고 있는 개인정보의 정보주체 수 ⑨ 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서 ⑩ 개인정보의 열람 요구를 접수처리하

는 부서 ⑪ 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유를 개인정보 보호위원회에 등록하여야 한다. 등록한 사항이 변경된 경우에도 또한 같다(법 제32조 제1항). 그런데 이 등록 및 공개 의무는 “범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일”에 대하여 적용되지 않는다(법 제32조 제2항 제2호). 이에 동반하여 범죄수사 및 형집행 등에 관련된 개인정보파일은 등록 개인정보파일에 대한 보호위원회의 개선 권고(법 제32조 제3항) 및 공개(법 제32조 제4항)의 대상에서도 제외된다.

또 개인정보 보호법은 모든 개인정보처리자에게 개인정보 처리방침의 수립 및 공개 의무를 규정하고 있는데, 다만 공공기관은 앞서 등록대상이 되는 개인정보파일에 대하여서만 개인정보 처리방침을 정하도록 하였다(법 제30조 제1항). 개인정보처리자는 ① 개인정보의 처리 목적 ② 개인정보의 처리 및 보유 기간 ③ 개인정보의 제3자 제공에 관한 사항(해당되는 경우) ④ 개인정보의 파기절차 및 파기방법(보존하는 경우 그 근거와 항목) ⑤ 개인정보처리의 위탁에 관한 사항(해당되는 경우) ⑥ 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항 ⑦ 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처 ⑧ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항 (해당하는 경우) ⑨ 처리하는 개인정보의 항목 ⑩ 개인정보의 파기에 관한 사항 ⑪ 개인정보의 안전성 확보 조치에 관한 사항 등이 포함된 개인정보 처리방침을 정하여야 하는데, 처음부터 등록대상이 되지 않은 범죄수사 및 형집행 등에 관련된 개인정보파일의 경우 법률적으로 개인정보 처리방침을 정할 의무조차 없는 것이다.

정보주체는 자신의 개인정보에 대하여 열람(법 제35조), 정정·삭제(법 제36조), 처리정지(법 제37조)에 대한 권리를 행사할 수 있으며, 자신 이외로부터 수집한 개인정보의 수집출처 등에 대하여 개인정보처리자로부터 고지받을 권리(법 제20조) 또한 보유하고 있다. 그러나 범죄수사 및 형집행 등에 관련된 개인정보파일의 경우 이러한 정보주체의 권리 행사가 제한되고 있다. 우선 정보주체가 공공기관에 대하여 열람을 요구할 때에는 공공기관에 직접 열람을 요구하거나 대통령령으로 정하는 바에 따라 요구할 수 있다(법 35조 제2항). 그런데 실무상 공공기관에 대한 개인정보 열람 요구는 국가 개인정보보호 포털(https://www. privacy.go.kr/)에서 신청하도록 하고 있는데, 이 열람은 공개되어 있는 개인

정보파일 목록 가운데 대상 개인정보파일을 지정해야만 가능하다. 결국 정보주체가 열람할 수 있는 공공기관의 개인정보파일은 법32조에 의해 등록 및 공개된 개인정보파일 목록에 한정되어 있으며, 동조 제2항 제2호에 의해 그 등록과 공개가 제외되어 있는 범죄수사 및 형집행 등에 관련된 개인정보파일은 정보주체의 열람권 행사가 어려운 것이다.

<그림6-1> 개인정보 열람등요구 신청화면

* 출처: 개인정보보호 포털(https://www.privacy.go.kr/) > 민원마당 > 개인정보 열람등요구

나아가 행정 고시인 표준 개인정보 보호지침에서는 개인정보의 제3자 제공 현황에 대한 열람청구를 받은 개인정보처리자에 대하여, 국가정보원 등 수사기관이 국가안보에 긴요한 사안에 대한 수사를 진행하고 있는 경우 제3자에 해당하는 당해 수사기관에게 열람청구의 허용 또는 제한, 거부에 관련한 의견을 조회하여 결정하도록 하였다(표준지침 제31조제2항 및 행정자치부, 2016: 308). 또 같은 지침 제44조(정보주체의 열람등 요구)에서는 영상정보처리기기를 운영하고 있는 공공기관이 범죄수사·공소유지·재판수행에 중대한 지장을 초래하는 경우라고 보는 경우 정보주체의 개인영상정보 열람등 요구를 거부할 수 있다고 규정하고 있다. 이와 같은 열람권의 제한은 법률에 명시되어 있지 않은 사

유이다.

이처럼 현행 개인정보 보호법과 관련 공공기관 실무에서는 범죄의 수사 및 형 집행 등과 관련하여 보유하고 있는 개인정보파일에 대한 정보주체의 열람권 행사를 광범위하게 제한하고 있다. 정보주체의 열람 요구가 범죄수사 및 형집행 등에 중대한 지장을 초래하는지를 개별적으로 살피지 않고 포괄적으로 제한하는 것은 정보주체가 자신의 권리에 대한 침해를 발견하고 구제를 받을 수 있는 가능성을 부당하게 가로막는다. 나아가 개인정보의 정정·삭제권은 자신의 개인정보를 열람한 정보주체가 행사할 수 있으므로(법 제36조) 자신의 개인정보를 열람하지 못한 정보주체는 그에 동반하는 정정·삭제 요구권도 제한받고 있다. 또 정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있지만(법 제37조), 공공기관의 경우에는 등록 대상이 된 개인정보파일 중에 포함된 자신의 개인정보에 대해서만 처리정지를 요구할 수 있고(법 제37조제1항), 그 등록과 공개가 제외되어 있는 범죄수사 및 형집행 등에 관련된 개인정보파일에 대해서는 처리정지권을 행사할 수 없다.

한편 개인정보 보호법은 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 개인정보의 수집 출처, 개인정보의 처리 목적, 개인정보 처리의 정지를 요구할 권리가 있다는 사실을 정보주체에게 알리도록 하였고, 5만명 이상의 민감정보나 100만명 이상의 개인정보를 처리하는 개인정보처리자가 정보주체 이외로부터 개인정보를 수집하여 처리하는 때에는 정보주체의 요구가 없어도 정보주체에게 고지하도록 하였다(제20조 제1항 및 제2항). 그러나 이 의무는 법 제32조 제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 개인정보에 대해서는 제외되기 때문에 범죄수사 및 형집행 등에 관련된 개인정보파일의 경우 정보주체의 고지받을 권리를 보장하지 않는다.

셋째, 경찰은 특별한 법령적 근거에 의하지 않고 여러 종의 정보통신시스템을 구축·운영하며 범죄수사와 관련한 개인정보파일을 상당히 방대하게 처리해 왔다. 이재정 의원의 국정감사에 따르면 2017년 현재 경찰청이 구축·운영 중인 개인정보처리시스템은 50개로서 보유하고 있는 개인정보는 36억여 건에 달한다[420]. 이중 실종아동시스템, 형사사

420) 이재정 의원 보도자료, 2017.10.14., “경찰 개인정보처리시스템 83개, 개인정보영향평가는

법정보시스템(KICS), DNA신원확인시스템(DIMS) 등 법률에서 구체적으로 정보시스템의 구축 및 운영에 관한 사항을 규정한 경우도 있었지만, 대부분의 경찰 정보시스템은 법령에 의해 구체적으로 규율되고 있다고 보기 어렵다. “치안정보의 수집·작성 및 배포 등” 등 경찰관직무집행법 및 경찰법 상 일반규정에 의한 경우가 10건, 개인정보 보호법의 일반규정 외에 다른 근거를 밝히지 못한 경우가 5건이었고, 정보주체의 동의에 의해 운영되는 경우가 6건이었다. 구체적인 법령적 근거를 갖추지 못한 시스템이 전체의 절반 가까이 되는 것이다. 경찰청이 밝힌 대부분의 법적 근거들은 해당 시스템의 구축・운영은 물론, 개인정보의 처리 목적, 대상 항목, 보유 및 이용 기간 등이 명확히 규율되고 있다고 보기 어렵다. 예를 들어 채증판독시스템의 경우, 그 법적 근거가 경찰법 제3조, 경찰관직무집행법 제2조, 형사소송법 제196조2항, 제199조1항, 개인정보 보호법 제15조 1항 3호라고 하였지만 이 규정들은 경찰의 치안 활동이나 수사 등 일반적인 직무에 대한 규정에 불과하다.

경찰정보시스템에 대한 이러한 법적 규율의 미비는 개인정보 보호법의 제정 이전에 이루어진 헌법재판소와 대법원의 과거 결정 및 판결에서 유래한 측면이 있다. 2005년 헌법재판소는 경찰청장이 지문정보를 보관하는 행위에 대하여 구체적인 법률에 근거하지 않아도 일반규정인 (구)공공기관의개인정보보호에관한법률[421] 제5조, 제10조 제2항 제6호에 근거한 것으로 볼 수 있고, 그 밖에 주민등록법 제17조의8 제2항 본문, 제17조의10 제1항, 경찰법 제3조 및 경찰관직무집행법 제2조에도 근거하고 있다고 보았다(헌재 2005. 5. 26. 99헌마513, 2004헌마190병합).

19건뿐!”, <https://blog.naver.com/leejjlaw/221117095023>.

421) (구)공공기관의개인정보보호에관한법률
제5조 (개인정보화일의 보유범위) 공공기관은 소관업무를 수행하기 위하여 필요한 범위 안에서 개인정보화일을 보유할 수 있다.
제10조 (처리정보의 이용 및 제공의 제한) ① 보유기관의 장은 다른 법률에 의하여 보유기관의 내부에서 이용하거나 보유기관 외의 자에게 제공하는 경우를 제외하고는 당해 개인정보화일의 보유목적 외의 목적으로 처리정보를 이용하거나 다른 기관에 제공하여서는 아니된다.
② 보유기관의 장은 제1항의 규정에 불구하고 다음 각 호의 1에 해당하는 경우에는 당해 개인정보화일의 보유목적 외의 목적으로 처리정보를 이용하거나 다른 기관에 제공할 수 있다. 다만, 다음 각 호의 1에 해당하는 경우에도 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그러하지 아니하다.
6. 범죄의 수사와 공소의 제기 및 유지에 필요한 경우

<표6-2> 경찰의 개인정보처리시스템 현황 (2017. 10.)

연번	시스템명	개인정보보유량	법적 근거
1	182경찰민원콜센터상담시스템	795,710	개인정보 보호법 제15조제1항
2	출입관리시스템	3,731	보안업무규정 제32조, 제46조
3	방문예약시스템	43,206	보안업무규정 제32조, 제46조
4	경찰박물관 인터넷홈페이지	883	정보주체 동의
5	경찰사이버교육포털	132,740	경찰공무원승진임용규정 제44조(대통령령)
6	경찰채용업무관리시스템	143,974	경찰공무원임용령 제51조(대통령령)
7	인사관리시스템	1,250,000	공무원인사기록통계및인사사무처리규정 제39조(대통령령)
8	전자공무원증관리시스템	130,000	경찰공무원임용령 시행규칙 12조 (대통령령)
9	폴복지시스템	328,490	공무원 후생복지에 관한 규정 제13조, 공무원보수등의 업무지침 제10장 맞춤형복지제도업무처리기준(640p)
10	경비업관리시스템	728,073	경비업법 시행령 제31조의2
11	스마트워크시스템	1,536,901	경찰관직무집행법 제2조, 개인정보 보호법 제15조제1항제3호

12	112신고시스템	19,567,155	경찰관직무집행법 제2조, 개인정보 보호법 제15조제1항제3호
13	즉심 및 통고처분시스템	4,197,915	경범죄처벌법 제7조, 제8조, 제9조, 시행령 제3조, 제4조, 제5조
14	총포화약 안전관리시스템	2,825,751	개인정보 보호법 제15조1항3호, 총포도검화약류등의안전관리에관한법률 시행령 제83조의2 사격장법 시행령 제12조, 제83조의2
15	유실물 종합관리시스템	6,773,370	개인정보 보호법 제15조제1항제1호, 제24조제1항제1호, 유실물법시행령 제13조
16	풍속업무 관리시스템	769,205	풍속영업의규제에관한법률 시행령 제9조, 제10조
17	사회적약자(실종아동시스템)	4,123,966	실종아동등의보호및지원에관한법률 제8조의2, 같은법 제7조의2, 시행령 제4조의2, 시행령 제8조의2, 실종아동등의발견및유전자검사등에관한규칙 제3조
18	117학교폭력신고시스템	294,041	개인정보 보호법 제15조제1항제3호, 학교폭력예방및대책에관한법률 제20조의2제1항
19	형사사법정보시스템(KICS)	2,740,833,963	형사사법절차전자화촉진법
20	범죄첩보분석시스템(CIAS)	127,759	경찰법 제3조, 경찰관직무집행법 제2조, 형사소송법 제196조2항, 개인정보 보호법 제15조1항3호, 수사첩보수집및처리규칙
21	의무경찰 복무관리시스템	236,807	의무경찰대설치및운영에관한법률 시행령 제61조의2
22	대한민국 의무경찰 홈페이지	35,120	의무경찰대설치및운영에관한법률 시행령 제61조의2
23	비상동보장치시스템	1,920	개인정보 보호법 제15조1항제1호
24	항공업무 전산시스템	151	개인정보 보호법 제15조 및 경찰관직무집행법 제10조 경찰헬기운용에따른운항,정비및항공종사자관리프로그램
25	채증판독시스템	627	경찰법 제3조, 경찰관직무집행법 제2조, 형사소송법 제196조2항, 제199조1항, 개인정보 보호법 제15조1항3호

26	신원업무통합관리시스템	23,581,456	국정원법 제3조, 보안업무규정 제33조
27	사이버경찰청 홈페이지	9,666	민원사무처리에 관한 법률 제8조, 사이버경찰청 운영규칙 775호
28	푸르미시스템	116,914	경찰공무원징계령
29	민원업무관리시스템	1,063,798	민원처리에관한법률시행령 제52조
30	경찰민원포털시스템	212,885	민원처리에관한법률시행령 제52조
31	피해자인권포털시스템(CARE)	17,633	범죄피해자보호법 시행령 제3조의2
32	경찰모바일시스템	151,032	개인정보 보호법 제15조
33	수배차량검색시스템	37,126,652	경찰관직무집행법 제2조제2호, 개인정보 보호법 제25조제1항제2호, 동법 제58조2항
34	스마트국민제보	1,146,518	공익신고자보호법 제8조
35	온라인조회시스템	91,084,344	경찰관직무집행법제2조, 동 시행령 제8조, 형의실효등에관한법률 제5조의2, 동 시행령, 자동차 관리법 제69조, 동 시행령 제14조, 개인정보 보호법 제15조1항2호
36	통합포털(폴넷)	151,283	개인정보 보호법 제15조
37	행정업무 사용자관리시스템	151,283	개인정보 보호법 제15조, 경찰정보통신운영규칙 제27조
38	경찰웹메일시스템	130,207	개인정보 보호법 15조 1항, 경찰청정보통신운영규칙, 경찰청정보통신보안업무규칙
39	원스톱장비포털	116,667	정보주체 동의

40	사이버범죄신고시스템(eCRM)	1,600,012	정보주체 동의
41	누리캅스	820	정보주체 동의
42	예방교육 신청시스템	680	정보주체 동의
43	교통경찰업무관리시스템(TCS)	535,136,421	도로교통법 제137조, 도로교통법 시행령 제87조의3
44	DNA신원확인시스템(DIMS)	60,421	디엔에이신원확인정보의이용및보호에관한법률 시행령 제3조
45	지문자동검색시스템(AFIS)	53,874,498	경찰관직무집행법시행령 제8조, 주민등록법시행령 제36조 주민등록법시행규칙 제8조, 출입국관리법시행규칙 제52조
46	전자 수사자료표시스템(E-CRIS)	19,647,758	경찰관직무집행법시행령 제8조, 형의실효등에관한법률 제2조제5조, 시행령 제2조제6조, 지문및수사자료표등에관한규칙 제2조제4조제5조,지문을채취할형사피의자의범위에관한규칙 제1조제2조
47	과학적 범죄분석시스템(SCAS)	1,420,953	경찰관직무집행법 시행령 제8조
48	지리적 프로파일링(GeoPros)	40,795,843	형사사법절차전자화촉진법 시행령 제18조, 경찰관직무직행법시행령 제8조
49	범죄경력관리시스템(CRIMS)	13,761,973	형의실효등에관한법률 제6조
50	3D얼굴인식시스템(FRS)	713,000	형의집행및수용자의처우에관한법률 제19조, 제87조, 경찰관직무집행법 제9조, 개인정보 보호법 제15조, 제18조, 범죄수법공조자료관리규칙 제3조, 제5조
합계		3,606,954,175	

* 출처: 이재정 의원 보도자료(2017. 10. 13).

재판관 송인준, 재판관 주선회, 재판관 전효숙은 반대의견에서 경찰법 제3조가 경찰청은 치안에 관한 사무를 관장한다는 경찰의 조직법이며 경찰관직무집행법 제2조는 경찰관의 일반적인 직무집행의 범위를 규정한 것에 불과하므로, 경찰청장이 구체적인 법률에 근거를 두지 않고 지문원지를 수집·보관하는 행위는 정보이용의 주체, 목적과 범위 등을 구체적으로 특정하여 규율하여야 할 개인정보 자기결정권의 본질에 반한다고 지적하였으나 소수에 그쳤다.

대법원도 앞서 헌재 결정과 유사한 취지의 판결을 하였다. 2009년 무혐의 처분을 받은 피의자의 사건정보를 경찰이 구체적인 법률에 근거를 두지 않고 경찰 범죄정보관리시스템이나 법무부 형사사법정보시스템에 기록·보관한 행위에 대하여 제기된 손해배상 청구소송에서, 대법원은 (구)공공기관의개인정보보호에관한법률 제5조가 공공기관이 소관업무를 수행하기 위해 필요한 범위 안에서 개인정보파일을 보유할 수 있도록 허용하고 있고, 치안정보의 수집, 작성 및 배포를 규정한 경찰법 제3조, 경찰관직무집행법 제2조 등에 근거하여 위 개인정보의 기록·보관이 위법하지 않다고 보았다(대법원 2012.10.25. 선고 2012다12641 판결).

그러나 2011년 제정 시행된 개인정보 보호법은 (구)공공기관의개인정보보호에관한법률과 달리 공공기관의 경우에도 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 또는 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우에 한하여 개인정보의 수집·이용을 허용하고 있다(개인정보 보호법 제15조 제1항 제2호 및 제3호). 그럼에도 여전히 많은 경찰의 정보시스템이 법령상 또는 업무 수행의 불가피성을 따지지 않고 개인정보 보호법, 경찰법, 경찰관직무집행법의 일반규정에 근거를 두고 구축 및 운영되고 있는 것이다. 경찰이 방대한 양의 개인정보를 특별한 조건이나 절차적 제한 없이 계속하여 처리하고 향후 빅데이터 분석 및 자동화된 의사결정에까지 이른다면 국민의 개인정보 자기결정권에 대한 부당한 제한이 아니라 할 수 없다.

경찰정보시스템이 사전적으로나 사후적으로나 아무런 통제를 받고 있지 않은 상황은 일차적으로 입법적으로 해결되어야 마땅하다. 정보시스템과 이를 통한 자동화된 처리에 대해서는 그 각각의 목적, 대상, 범위 및 통제에 대하여 법률적으로 구체적인 규정을 두어 규율하는 것이 바람직하다. 비록 소수 의견이기는 하지만 앞서 헌재 2005. 5. 26. 99

헌마513, 2004헌마190병합 결정에서 재판관 송인준, 재판관 주선회, 재판관 전효숙은 경찰이 정보이용의 주체, 목적과 범위 등을 구체적으로 특정하여 법률적으로 규율하는 것이 바람직하다고 보았다. 헌재 2005. 7. 21. 2003헌마282 등 결정에서 재판관 권성 또한 반대의견에서 정보처리시스템은 정보처리 방식의 면에서 개인정보 자기결정권에 대한 제약의 정도가 대단히 큰 방식인 바, 이러한 방식의 개인정보 처리가 정당화되려면 처리되는 정보의 범위가 최소화되어야 할 뿐만 아니라 개인정보의 처리목적이 수집단계에서 명확히 특정되어 있어야 하고 또한 그 특정 목적에 따라서만 해당 정보를 저장・이용・전달 등의 처리를 할 것이 요구된다고 지적하였다. 유럽인권재판소는 2000년 Rotaru v. Romania 사건에서 국가 감시 조치의 대상이 되는 정보의 유형, 감시 대상이 되는 사람들의 범주, 감시 조치가 취해질 수 있는 상황 또는 절차를 규정하지 않은 것이 유럽인권협약 제8조 위반이라고 결정하였다. 경찰개혁위원회 또한 2018년 경찰 정보시스템 구축과 운영에 대해서는 그 근거, 절차와 방식 및 통제에 관한 별도의 구체적인 법률상 근거를 마련하고, 경찰 내외부에 공개하지 않는 정보시스템의 구축운영 금지 등을 권고하였다[422].

422) 경찰개혁위원회(2018), 경찰의 정보활동 개혁 권고(연번 25).

제7장 국가인권기구와 개인정보 보호

국가인권기구의 개인정보 보호 업무의 성격을 검토함에 앞서 개인정보 보호의 감독에 대한 국제 규범 및 국내 감독 체계와 그 한계를 살펴본다.

제1절 개인정보 보호 감독의 규범

1. 개인정보 보호 감독 국제규범의 발전

가. 개인정보 보호 감독 국제규범의 수립

한 국가의 개인정보 보호 감독체계는 일반적으로 개인정보 보호법의 준수를 감독하는 법제도 및 기관을 아우르는 개념으로, 국제적으로 여러 규범에서 독립적이고 효과적인 하나 이상의 개인정보 보호 감독기관(Data protection authorities)의 설치를 권고하고 있다. 대개의 국가에서 개인정보 보호 감독기관은 개인정보 보호법을 소관하고 집행하며 관련 지침을 제공하는[423] 공공기관이자, 법적으로 독립적이면서 여러 기능을 갖춘 다면적인 규제기관이다[424]. GDPR에서 개인정보 보호 감독기관은 "개인정보 처리와 관련하여 자연인의 기본권과 자유를 보호하고 유럽연합 내에서 개인정보의 자유로운 흐름을 촉진하기 위해 본 규정의 적용을 모니터링하는 하나 또는 그 이상의 독립적 공공기관"이다(GDPR 제51조제1항).

개인정보 보호 감독체계에 대한 국제규범이 등장한 것은 컴퓨터를 비롯한 현대 정보통신기술의 발달로 개인정보의 처리가 자동화됨에 따라 보다 적극적으로 개인정보 보호 관련 법률과 규제체계를 수립할 필요성이 확인되었기 때문이다. 특히 개인정보 보호 체계에서 독립적인 감독기관이 요청되는 이유는 공공기관에 대한 감독과 효과적인 규제 측면에서 살펴볼 수 있다[425]. 전통적으로 정부기관이나 대기업들이 개인정보를 대량으로

423) Gabel, Detlev and Hickman, Tim(2016), "Chapter 14: Data Protection Authorities" in Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law. White & Case LLP, <https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation>.

424) Barnard-Wills, David and Wright, David(2014), "PHAEDRA : Improving Practical and Helpful co-operAtion bEtween Data pRotection Authorities", p.10.

처리하는 상당부분을 차지하였고, 이들의 개인정보 처리에 대해서 전문적으로 평가·견제할 수 있는 장치가 필요했다. 따라서 감독자와 피감독자가 조직적·기능적으로 분리되어 있는 것이 중요하다[426]. 또 개인정보 보호 감독기관이 효과적이기 위해서는, 감독기관이 믿을 수 있는 규제자(credible regulator)라는 점에 대해 시민과 기업의 신뢰가 확보되어야 한다. 투명하고 공정한 임명과 면직절차는 감독기관이 조직적으로 자율적이라는 점을 보증할 수 있고 그리하여 이해관계자들로부터 신뢰를 확보할 수 있다(이인호 외, 2017 : 42).

유엔은 1990년 결의한 <전자화된 개인정보파일의 규율에 관한 지침>[427]에서 감독과 제재(Supervision and Sanctions)에 대한 원칙(8)을 명시하고 모든 국가들이 이 지침에 열거된 원칙의 준수를 감독하는 기구를 국내 법률 체계에 따라 법적으로 설치하도록 권고하였다. 이 기구는 공정해야 하고 개인정보의 처리 및 생성을 소관하는 독립적인 개인 또는 기관으로서 기술적인 역량을 갖추어야 한다. 이 원칙을 이행하는 국내법 규정을 위반하는 일이 발생한 경우 형사상 또는 기타 처벌과 함께 적절한 개인 구제가 강구되어야 한다.

유럽연합은 개인정보 보호 감독체계를 보다 법률적인 수준으로 수립하였다. 자동화된 방식 또는 체계적 개인정보파일 형태로 개인정보를 처리하는 경우가 늘면서 유럽연합 각국이 다양한 방식으로 이에 대응하는 입법에 나섰고, 유럽연합은 역내에서 더 조화롭고 일관된 개인정보 보호 법체계를 마련하고자 개인정보 보호 디렉티브를 추진하였다(Hustinx, 2013: 2). 1995년 채택된 <개인정보 처리 및 정보의 자유로운 이동에서 개인의 보호에 관한 유럽의회 및 정상회의 디렉티브'(Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 일명 '개인정보 보호 디렉티브')>는 특히 완전히 독립적인 감독을 위한 기구 설립 및 감독 시행을 법적으로 의무화하였다. 개인정보 보호 디렉티브는 서문에서 개인정보 보호 감독기관이 개인

425) Schutz, Philip(2012), Comparing formal independence of data protection authorities in selected EU Member States, Conference Paper, ECPR Standing Group on Regulation & Governance (Biennial Conference) <4, 2012, Exeter>, p3.

426) 권건보 외(2017), 앞의 글. p96.

427) Guidelines for the Regulation of Computerized Personal Data Files, G.A. res. 44/132, 44 U.N. GAOR Supp. (No. 49) at 211, U.N. Doc. A/44/49 (1989).

정보의 처리에 관하여 개인을 보호하기 위한 본질적 요소(essential component)라고 선언하고(서문 62) 제28조(감독기관)에서 각 회원국이 디렉티브 이행 법률에 포함해야 할 감독기관 관련 사항을 상세히 규정하였다. 개인정보 보호 감독기관은 소관 업무를 완전히 독립적으로 수행할 수 있어야 하고, 각국 관련 행정 조치나 정책에 대한 자문권을 가지며, 조사권, 효과적인 개입권, 고발권을 비롯한 권한을 행사할 수 있어야 하고, 진정 사건을 처리하도록 했다.

이후 유럽연합은 2000년 기본권헌장(Charter of Fundamental Rights of the European Union) 제8조 및 2007년 유럽연합의 운영에 관한 조약(Treaty on the Functioning of the European Union, TFEU) 제16조에 기존의 사생활권과 별도로 개인정보 보호권을 기본권으로 명시하고 독립적인 기관에 의한 개인정보 보호 감독에 대하여 규정하였다. 이는 독립적인 감독의 원칙 및 감독기관의 설치가 유럽 수준에서는 개인정보 보호에 대한 권리의 본질적 요소이자 헌법적 요소로 발전하였음을 의미한다. 개인정보 보호 감독은 개인정보 보호 원칙에 대한 준수를 보장하려는 임무를 띠고 있으며, 개인정보의 효과적인 보호 체계에 대한 문제와 맞닿아 있다(Hustinx, 2013: 4)[428].

2010년 유럽사법재판소 판결[429]은 개인정보 보호 감독기관의 활동이 객관적이고 공정하게 이루어지기 위한 조건으로 정부로부터 분리를 요구하였다. 왜냐하면 정부는 그 자신이 '한 쪽의 이해당사자'가 될 수 있고, 정부 자신의 다른 기능들(특히, 과세 혹은 법집행)을 수행하기 위한 목적에서 개인정보 보호법을 무시할 수 있기 때문이다. 유럽기본권청(FRA)에 따르면 개인정보 보호 감독기관이 완전한 독립성을 가지고 기능하는 것에 대한 법적 요건은 피감독 기관들로부터의 영향 뿐 아니라, 국가나 지방정부의 직접 또는 간접적인 영향을 포함하여 어떠한 외부적 영향력으로부터도 자유로워야 함을 의미한다[430].

한편 유럽평의회는 1981년 <개인정보 보호 협약(일명 '108호 협약')>에 대한 2001년 추가 의정서[431]에서 조인국들에게 독립적인 개인정보 보호 감독기관의 설립을 의무화하

428) Peter J. Hustinx(2013), (Future) Interaction Between Data Protection Authorities and National Human Rights Institutions, in the National human rights institutions in Europe : Comparative, European and International Perspectives, pp157-172.
429) CJEU(2010), C-518/07, European Commission v. Federal Republic of Germany [GC], 이인호 외(2017), 앞의 글, p.39 재인용.
430) FRA(2018a) op. cit., p192.

였다. 유럽평의회는 추가의정서 해설서에서 유럽연합 개인정보 보호 디렉티브의 경우와 마찬가지로 개인정보 보호 감독기관이 "민주사회에서 개인정보 보호 감독체계의 본질적인 요소"라고 규정하였다[432].

유럽 국가들이 개인정보 보호 감독체계를 강화해온 것은 개인정보 처리가 전례 없이 점점 더 복잡해져서 개인이 이해하기 어려워졌기 때문이다. 이러한 상황에서 유럽의 개인정보 보호 감독기관들은 디지털 시대 감시자(the watchdogs of the digital age)의 역할을 기대 받으며, 특히 유럽사법재판소는 완전히 독립적인 개인정보 보호 감독기관을 기본권의 '수호자'(the guardians)로 지칭하였다[433]. 또한 기본권청은 개인정보 보호 감독기관의 독립성이 국가 개인정보 보호 시스템에 대한 국민의 신뢰 측면에서 중요하다고 지적하였다. 개인정보 보호 감독기관의 독립성에 대한 의구심이 계속되거나 감독기관들이 주어진 임무를 효율적이고 효과적으로 수행하기에 충분한 자원을 확보하고 있지 못한 것처럼 보인다면, 국민들은 개인정보 보호나 프라이버시에 대한 자신들의 우려가 진지하게 다루어지고 있다고 믿지 못할 것이다[434].

독립적인 감독이 효과적인 개인정보 보호를 위해 필수적이라는 사실이 확인되면서 경제협력개발기구(OECD) 역시 2013년 프라이버시 가이드라인에서 "그 권한을 효과적으로 행사하는 한편, 객관적이고 공정하고 일관된 기준으로 의사결정을 내리기 위해 필요한 거버넌스, 자원 및 기술적 전문성을 갖춘 프라이버시 집행 기구를 설립하고 운영할 것"을 회원국에 권고하였다[435].

유엔은 특히 2013년 6월 미국과 영국 등 일부 국가의 정보기관들이 구글 등 통신·인터넷 기업들의 협조를 받아 세계 이용자의 개인정보 및 통신정보를 수집하고 공유해 왔

---

431) Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows(2001), Strasbourg.

432) Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows(2001), Strasbourg, para.5.

433) FRA(2018a), op. cit., pp189-192.

434) European Union Agency for Fundamental Rights(FRA)(2010b), Data Protection in the European Union: the role of National Data Protection Authorities: Strengthening the fundamental rights architecture in the EU II. p50.

435) OECD(2013) Guidelines on governing the Protection of Privacy and transborder flows of personal data, Art. 19.

다는 사실이 폭로된 후, 국제인권법에서 보호해 온 '프라이버시권'을 디지털 시대 더욱 체계적으로 보호할 것을 각국에 요청해 왔다. 2013년 12월 유엔 총회는 국가의 통신 감시, 감청 및 개인정보 수집에 대해 적절한 투명성과 책무성을 보장할 수 있는 독립적이고 효과적인 국내 감독 체계를 설립하거나 운영할 것을 요청하였다[436]. 유엔 인권이사회 역시 2017년 3월 22일 <디지털시대 프라이버시권 인권이사회 결의안>을 통하여 독립적이고 효과적일 뿐 아니라 적절한 자원을 갖추고 공정한 국내 감독 체계를 사법부, 행정부, 또는 국회 하에 설립하거나 운영할 것을 요청하였다[437].

유엔 인권최고대표는 2014년 펴낸 <디지털시대 프라이버시권 보고서>에서 국가와 민간 플랫폼의 감시 문제에 대응하기 위하여 독립적이고 효과적인 감독기관의 역할이 중요하다고 강조하였다[438]. 디지털 시대 커뮤니케이션 기술은 정부, 기업, 개인이 감시, 도청, 개인정보 수집을 실행할 수 있는 능력 또한 향상시켜 왔다. 특히 국가는 동시적, 침투적, 표적적이거나 광범위한 감시를 수행할 수 있는 능력을 그 어느 때보다 막대하게 보유하게 되었으며, 세계 정치경제사회가 깊이 의존하고 있는 기술 플랫폼은 대량 감시에 취약할 뿐 아니라 이를 촉진하는 환경이다. 이런 상황에서 독립적이고 외부적인 감독이 부재한 내부적 안전 조치는 불법적이고 자의적인 감시 방식에 대해 전혀 효과적이지 않은 것으로 나타났다(동보고서 para.37).

많은 국가의 개인정보 보호법이 범죄수사 및 국가정보 활동 부문을 예외로 규정하고 있는 현실 속에서, 이러한 유엔의 접근은 수사기관 및 정보기관의 개인정보 수집 활동을 개인정보 보호 규범 안으로 부분적으로 포함할 것을 요청하고 있다는 데 의의가 있다.

나. 유럽의 개인정보 보호 감독 강화

1) GDPR의 개인정보 보호 감독 강화

개인정보 보호 감독에 대한 국제규범을 적극적으로 주도해 온 유럽은 유럽연합과 유럽평의회의 관련 규범을 일치시켜 가면서 유럽 지역 내 개인정보 보호 감독이 같은 방

436) The right to privacy in the digital age, Resolution adopted by the General Assembly on 18 December 2013, 68/167.
437) UN Human Rights Council (2017), The right to privacy in the digital age. A/HRC/34/L.7/Rev.1.
438) UN High Commissioner for Human Rights(2014), op. cit.

식으로 작동하게끔 노력하였다[439]. 그러나 유럽연합 회원 각국이 개인정보 보호 디렉티브에 따라 마련한 국내 이행 법률들 간 차이로 인해 감독기관들의 집행 방식이 상당히 다양한 것으로 나타났다. 유럽 기본권청 및 유럽사법재판소가 그 불일치와 결점을 잇따라 지적하자 유럽연합 집행위원회는 개인정보 보호 개혁 패키지를 마련하였다(Hustinx, 2013: 7).

2016년 5월 24일 발효한 유럽연합 개인정보 보호 개혁 패키지(EU Data Protection Reform package)[440]는 두 가지 법안을 포함하고 있다. 그 중 하나는 '유럽 개인정보 보호법'으로 소개되기도 하는 GDPR이다. '규정'이 유럽연합 회원국에 직접 구속력을 갖는다는 점에서 이 제안은 유럽 전체적으로 개인정보 보호에 대한 포괄적 입법체계와 통합형 수행체계를 마련한 것으로 평가된다. 개혁 법안의 다른 하나는 <형사 법집행 목적의 개인정보 보호에 대한 디렉티브(directive on protecting personal data processed for the purpose of criminal law enforcement, 일명 '경찰 디렉티브')>이다.

GDPR은 개인정보 보호 감독기관에 대하여 제6장(독립적 감독기관)에서 제51조(감독기관), 제52조(독립성), 제53조(감독기관 구성원에 대한 일반 조건), 제54조(감독기관 설립에 관한 규칙), 제55조(주무 권한), 제56조(지휘 감독기관의 주무 권한), 제57조(업무), 제58조(권한), 제59조(활동 보고서)에 걸쳐 감독기관의 독립적 지위 및 주무 권한, 업무 및 권한에 대하여 구 개인정보 보호 디렉티브보다 훨씬 더 상세한 규정을 두었다. 나아가 제7장(협력과 일관성)에서도 제60조(주감독기관와 다른 관련 감독기관의 협력), 제61조(상호 지원), 제62조(감독기관 공동 작업), 제63조(일관성 메커니즘), 제64조(EDPB 의견), 제65조(EDPB에 의한 분쟁 해결), 제66조(긴급 절차), 제67조(정보 교환) 등에서 국내 및 유럽연합 감독기관 간 협력과 일관성 체계에 대하여 규정하였다.

개인정보 보호 감독기관에 대한 GDPR 규정을 개인정보 보호 디렉티브에 따른 규율과 비교하여 보았을 때 여러 면에서 주요한 변화가 있었다고 평가받는다(이인호 외, 2017: 131~143). 우선 독립성 면에서 GDPR은 기본적으로 개인정보 보호 디렉티브 요건을 따르고 있지만 독립성 요건을 훨씬 더 구체적으로 규정하였으며, 감독기관의 설립 및 구성, 설립에 대한 규칙 등이 법률상으로 강화되었다. 직무와 권한 또한 GDPR에서 훨씬 더 상

439) FRA(2018a), op. cit., p191.
440) "Data protection reform", (검색일: 2020. 9. 1.)
<https://www.consilium.europa.eu/en/policies/data-protection-reform/>

세하게 규정하고 강화하였다. 특히 여러 회원국에 걸쳐 영업을 하는 기업들에 대하여 역내 집행체계를 일원화하는 한편, 감독기관 간 협력 및 차이에 대한 해결 규정을 두고 있는 점이 두드러진다. 즉, 주감독기관(lead supervisory authority)을 통한 원스톱 집행체계를 갖추는 한편으로, 주감독기관과 다른 관련 감독기관 간의 협력 및 감독기관 간 공동작업(joint operations)의 근거 규정을 두었다. 유럽연합 감독기관들의 협력 체계로 EDPB를 두고 감독기관 간 분쟁 해결은 EDPB를 통하도록 하는 등 통일적 법적용 체계도 갖추었다.

한편, 경찰의 개인정보 처리는 관련된 사람에게 중대한 영향을 미치기 때문에 이 분야 개인정보 처리에 대한 보호 규율을 상세하게 규정하는 것이 필수적으로 요구된다[441]. 유럽연합 개인정보 보호 개혁 패키지에서 가장 눈에 띄는 변화 중 하나는 일부 예외를 제외하고 법집행 분야에도 원칙적으로 개인정보 보호 원칙을 적용한 것이다. 경찰 디렉티브는 회원국의 국내 이행 입법이 필요하다는 점에서 그 구속력이 GDPR과 차이가 있지만 GDPR과 마찬가지로 독립 감독기관을 의무화하고 있다.

유럽연합은 1995년 개인정보 보호 디렉티브 이후 각국 개인정보 보호 법체계에서 범죄수사 및 형집행 등 법집행 영역에 대해서 예외를 두어 왔다[442]. 개혁 법안은 경찰 디렉티브를 포함하여 이 문제를 개선하고자 하였다. 경찰 디렉티브는 GDPR에 비해 일부 규정이 완화되어 있지만 경찰 등 법집행 기관에 대해서도 원칙적으로 개인정보 보호 원칙 및 독립적인 감독을 적용하도록 하였다는 점에서 개인정보 보호 감독을 강화하였다.

그러나 앞서 제6장에서 살펴보았듯이 경찰 디렉티브의 경우 GDPR에 비해 감독기관의 권한 및 정보주체의 권리구제와 관련된 일부 규정이 완화되어 있다. 감독기관의 업무와 권한의 제한은 법집행기관의 특수성 측면에서 이해되는 측면이 있다. 그러나 GDPR에 비해 완화된 감독 규정으로 인해 컨트롤러로서 법집행기관의 책임성 보장과 감독기관의 효과적 감독에 중대한 지장이 초래되지 않았는지 추후 평가를 지켜볼 필요가 있다.

한편, 유럽평의회의 경우 개인정보 처리 관련 규범에서 경찰 및 형사사법을 포함한 모든 분야를 망라하고 있다는 점에서 유럽연합과 차이를 보이고 있다.

---

441) FRA(2018a), op. cit., p277.

442) 개인정보 보호 디렉티브는 경찰 및 형사사법분야에는 적용되지 않는다. European Union Agency for Fundamental Rights, Council of Europe(2014), Handbook on European data protection law, p149.

2) 108호 협약 현대화 및 경찰 권고의 감독 강화

유럽연합이 GDPR 등 개인정보 보호 법체계 개혁에 나서는 한편으로, 유럽평의회 역시 2018년 5월 18일 기존의 108호 협약을 '현대화된 108호 협약'(The Modernised Convention)으로 개정하여 회원국 개인정보 보호 감독체계를 강화하였다[443].

현대화된 108호 협약은 기존의 추가의정서에 기초하여 감독기관의 권한 목록을 보완하였다. 개인정보 보호 침해에 대한 개입권, 조사권, 사법 기관 고발 및 소송에 개입할 권리에 더하여 감독기관은 정보주체, 컨트롤러, 프로세서 등 관련된 모든 참여자들의 이해를 증진하고, 정보를 제공하고, 교육할 의무가 있다. 감독기관의 결정권 및 제재권도 허용한다. 현대화된 108호 협약은 감독기관이 그 업무와 권한을 행사하는 데 있어 독립적이어야 한다는 점을 재차 강조하였다[444]. 협약 조인국의 이행을 평가할 때는 정보주체가 사용할 수 있는 다른 구제조치들과 함께 감독기관의 역할에 대하여 살펴보아야 한다[445].

유럽평의회와 유럽연합의 개인정보 보호 법체계 간 중요한 차이 중 하나는 유럽평의회의 경우 법집행 분야에도 적용된다는 점이다[446]. 유럽평의회 108호 협약은 개인정보 처리와 관련하여 경찰 및 형사사법을 포함한 모든 분야를 망라하고 있다. 유럽평의회는 이 점을 분명히 하고 1987년 '경찰 권고(police recommendation)'[447]를 채택하여 회원국들에게 개인정보 보호 관련 108호 협약의 원칙을 경찰의 개인정보 처리에도 적용할 것을 권장하였다. 2018년 유럽평의회는 현대화된 108호 협약을 개정하면서 <경찰 분야에서의 개인정보 사용에 관한 실질적 지침>[448]을 채택하여 경찰 권고를 보완하였다.

1987년 <경찰 권고>는 경찰의 개인정보 처리가 반드시 국내 개인정보 보호법에 대한 준수를 보장하는 독립적인 감독을 받도록 하였다. 정보주체는 108호 협약에 포함된 열람권을 보장받아야 한다. 감독기관과 관련하여서는 특히 원칙1(통제 및 통지)에서 '독립적

443) The amending Protocol (CETS No. 223) to Convention 108.
444) Council of Europe(2018), "The modernised Convention 108: novelties in a nutshell", <https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8>.
445) Council of Europe(2018), Explanatory Report, Convention 108 +: Convention for the protection of individuals with regard to the processing of personal data, para.35.
446) FRA(2018a), op. cit., p273.
447) Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector.
448) Practical Guide on the use of personal data in the police sector(2018).

인 감독기관'을 경찰 외부에 두도록 하고 권고에서 규정하는 개인정보 처리에 대하여 통제하고 감독하도록 하였다. 또 이 권고의 적용에서 문제가 발생하는 자동화된 처리 수단을 도입할 때 사전에 감독기관의 자문을 거치도록 하고 영구적인 자동화 파일에 대해서는 감독기관에 통지하도록 하였다. 원칙5(개인정보 전달)에서는 제3의 공공이나 민간기관에 개인정보를 전달할 때 법적 의무 또는 근거를 갖추거나 감독기관의 승인을 받도록 하였다. 목적 외로 개인정보파일을 결합시키거나 온라인으로 접근하려면 감독기관의 승인을 받아야 한다. 원칙6(경찰 파일의 공개 및 접근권, 정정권, 이의신청권)에서는 개인정보파일의 공개 및 그에 대한 열람 등 정보주체의 권리 행사를 보호할 수 있는 이의신청 수리 등 조치를 취하도록 하였고, 원칙7(개인정보 보관기간 및 갱신)에서는 서로 다른 분류의 개인정보에 대한 보관 기간을 수정하거나 개인정보 품질에 대한 정기 점검을 수정하는 규칙의 경우 감독기관과 합의하거나 법률에 따르도록 하였다.

2018년 <경찰 분야에서의 개인정보 사용에 관한 실질적 지침>은 '19. 외부통제(External control)' 원칙에서 하나 이상의 독립적이고 효과적인 감독기관을 두도록 의무화하였다. 이때 부처 또는 경찰 자체 내에 설립된 감독기관은 명확히 배제하였다[449].

108호 협약은 개인정보 보호를 위한 구속력 있는 유일한 국제협약으로서 유럽평의회 회원국이 아닌 국가에게도 가입을 열어두고 있다. 현재 한국은 108호 협약에 이미 옵저버로 가입되어 있는데, 국제 규범과의 조화를 위해서는 108호 협약에 정식으로 조인할 필요가 있다.

2. 국내 개인정보 보호 감독 체계와 한계

현재 국내 개인정보 보호 주감독기관으로는 국무총리 소속 개인정보 보호위원회를 들 수 있다. 개인정보 보호위원회는 2011년 개인정보 보호법이 제정되면서 대통령 소속의 합의제 행정기관으로 설립되었으나 감독의 독립성과 권한 미비 문제가 불거져 왔다. 2012년 국가인권위원회는 개인정보 보호위원회가 국제적 표준에 부합하는 직무상 독립성을 갖추고 있지 못하다고 지적하였고[450], 2016년 유럽연합 집행위원회는 우리나라 개

449) "The supervisory authority set up within a ministry or the police itself does not fulfil this obligation."

450) 국가인권위원회는 <2012~2016 국가인권정책기본계획(NAP) 권고안>에서 "개인정보

인정보 보호법에 대한 적정성 평가에서 감독기관이 부적격하다고 통보하였다.

개인정보의 오·남용 및 유출 등을 감독할 감독기관을 개인정보 보호위원회로 일원화한다는 취지[451]로 개인정보 보호법, 정보통신망법, 신용정보법 등 이른바 '데이터 3법'이 동반 개정되었다. 이로써 기존에 행정안전부, 방송통신위원회, 금융위원회에 분산되어 있던 법령 개선이나 정책 수립·집행, 개인정보 침해에 관한 조사·처분 권한을 대체로 개인정보 보호위원회로 일원화하였다. 2020년 8월 5일, 개정된 개인정보 보호법이 시행되면서 개인정보 보호위원회가 독자적인 조직·인사·예산의 운영 권한을 갖는 국무총리 소속의 장관급 중앙행정기관으로 격상되었다. 그러나 현행 개인정보 보호 감독체계는 여전히 다음과 같은 규제 사각 지대를 방치하고 있다는 점에서 한계가 있다.

가. 금융기관 개인정보 처리의 감독 분리

개정 개인정보 보호법 및 신용정보법에 따르면 금융회사는 개인정보 보호위원회의 감독 대상에서 제외된다. 개정 신용정보법은 "금융회사 등을 제외한 신용정보제공·이용자인 상거래기업 및 법인"에 대해서만 금융위원회의 감독, 금융감독원의 검사 등을 대신하여 개인정보 보호위원회에 자료제출요구·검사권·출입권·시정명령, 과징금 및 과태료 부과 등의 권한을 부여하였다[452]. 신용정보법의 주요 수범자인 금융회사는 금융위원회의 감독을 받는 것이다.

신용정보의 이용과 보호를 동시에 소관하고 있는 금융위원회는 독자적인 중앙행정기관이기는 하지만 개인정보 보호 감독 기능이 매우 취약하다. 신용정보법의 소관부서인 금융위원회 '데이터정책과'는 한 부서에서 ① 금융분야 데이터 활용에 관한 정책의 수립·총괄 ② 신용조회업·신용조사업·채권추심업에 관한 정책의 수립 및 제도개선 ③ 신용조회회사·신용조사회사·채권추심회사에 대한 인가·허가·감독 ④ 신용조회회사·금융회사의 개인신용평가 체계에 관한 정책의 수립 ⑤ 신용정보의 집중관리·활용에 관한 정책의 수

보호위원회는 실질적으로 심의, 의결기능만을 담당하고 실질적인 개인정보 보호 정책 수립, 개인정보 수집자 감독, 개인정보 침해 구제 업무는 행정안전부에서 담당하여 사실상 독립적인 기구로 보기 어려움"이라고 지적하였다.

451) 개인정보 보호법 일부개정법률안(인재근의원 대표발의), "제안이유", 2018. 11. 15.(의안번호: 2016621).

452) 신용정보의 이용 및 보호에 관한 법률 일부개정법률안(김병욱의원 대표발의), "주요내용", 2018. 11. 15.(의안번호: 2016636).

립 ⑥ 신용정보집중기관 및 신용정보협회에 대한 허가·감독 ⑦ 금융분야 빅데이터에 관한 정책의 수립 및 제도개선 ⑧ 빅데이터 분석시스템의 구축·운영·활용의 지원 ⑨ 금융분야 개인정보 보호 및 정보보안에 대한 정책의 수립 ⑩ 개인신용정보 침해 방지대책의 수립 및 금융분야 개인정보 보호에 대한 실태점검 ⑪ 금융분야 개인정보 보호 및 정보보안 관련 협의체의 운영 및 유관기관 감독 ⑫ 금융분야 데이터 활용, 정보보호, 신용정보업 및 신용정보집중기관에 관한 국제협력 ⑬ 제1호부터 제12호까지와 관련된 사항에 대한 조사·연구 ⑭ 제1호부터 제12호까지에 해당하는 금융관계 법령 및 규정의 제·개정에 관한 사항 ⑮ 제1호부터 제14호까지와 관련된 금융감독원의 업무에 대한 위원회의 지도·감독에 관한 사항 등의 업무를 동시에 주무한다. 이 부서는 그 업무에 금융분야 데이터 활용과 보호가 혼재되어 있어 방대한 금융분야 개인정보 처리에 대한 업무를 소관하기에 충분한 전문성과 독립성을 갖추었다고 보기 어려운 것이다.

무엇보다 금융위원회처럼 업종별 규제기관이 개인정보 보호와 충돌하는 업무를 함께 수행하는 경우 소관 행정부처와 관련 업계의 이해관계나 압력으로부터 자유롭지 못할 가능성이 높다(이인호, 2017: 118). 금융위원회는 데이터를 활용하고자 하는 금융기관, 즉 피감독기관으로부터 독립적으로 감독 기능을 발휘하기 어려울 수 있는 것이다. 결과적으로 금융기관의 개인정보 처리의 경우 독립적이고 효과적인 개인정보 보호 감독 하에 있다고 볼 수 없다.

따라서 효과적이고 독립적인 개인정보 보호 감독체계를 수립하기 위하여 신용정보법의 개인정보 관련 조항을 개인정보 보호법으로 일원화하고 금융위원회의 개인정보 감독 권한을 개인정보 보호위원회로 이관하는 것이 바람직하다.

나. 국가안전보장 관련 개인정보 처리의 포괄적 제외

현행 개인정보 보호법은 국가안전보장과 관련한 개인정보 처리에 대해서 포괄적으로 그 적용을 제외하는 규정을 두고 있다. “국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보”의 경우 개인정보 보호법 제3장부터 제7장까지를 적용하지 않는다(제58조 제1항 제2호). 다만 그 경우에도 개인정보처리자는 목적을 위하여 필요한 범위에서 최소한의 기간에 최소한의 개인정보만을 처리하여야 하며, 개인정보

의 안전한 관리를 위하여 필요한 기술적·관리적 및 물리적 보호조치, 개인정보의 처리에 관한 고충처리, 그 밖에 개인정보의 적절한 처리를 위하여 필요한 조치를 마련하여야 한다(제58조 제4항).

개인정보 보호위원회도 군이나 국가정보원의 개인정보 처리에 대한 그간의 결정에서 제58조 제1항 제2호에 의한 제외를 포괄적으로 인정해 왔다. 개인정보 보호위원회는 울산광역시 및 자치구에서 재난관측 및 산림·방범·교통·홍수 관리 등을 목적으로 설치한 영상정보처리기기를 통해 CCTV 통합관제센터에서 수집한 영상정보를 통합방위종합상황실에서 통합방위작전 지원을 위해 이용하고 제공받을 수 있다고 본 의결에서, 「통합방위법」의 법령상 규정에 의하지 않고 개인정보 보호법 제58조 제1항 제2호를 포괄적으로 적용하였다(개인정보 보호위원회 2018. 10. 15. 의결 제2018-21-230호). 또 보령시와 군·경이 합동으로 운영하는 통합방위지원본부도 통합방위작전 지원을 위해 CCTV 통합관제센터가 관제하는 모든 목적의 영상정보처리기기로부터 수집한 영상정보를 개인정보 보호법 제58조제1항제2호에 의해 이용하고 검색할 수 있으며, 나아가 해당 영상정보처리기기를 조작할 수 있다고 보았다(개인정보 보호위원회 2019. 2. 25. 의결 제2019-04-044호). 개인정보 보호위원회는 군 지역책임부대가 마찬가지로 제58조 제1항 제2호에 의해 통합방위사태 선포, 경계태세 2급 이상 발령, 통합방위훈련(자체훈련, 지상협동훈련, 대침투 종합훈련, 후방지역 종합훈련), 정부훈련(을지태극연습 등), 한미연합연습(동맹연습 등), 테러 발생 시 등에서 지방자치단체로부터 소관 업무 수행을 위하여 필요한 범위에서 통합관제센터의 영상정보를 전용회선을 통해 제공받을 수 있다고 보았다. 나아가 통합방위사태 선포, 경계태세 2급 이상 발령 시에는 지역책임부대가 지방자치단체 통합관제센터의 영상정보처리기기를 직접 조작할 수 있다고 보았다(개인정보 보호위원회 2019. 7. 22. 의결 제2019-14-222호)[453].

한편 개인정보 보호위원회는 경찰청이 국토교통부로부터 제공받는 차적자료를 다른 수사기관에 제공하는 문제에 관한 의결에서, 다른 법률에 특별한 규정이 있는 경우를 제외하고 개인정보를 제공받은 자의 재제공을 금지하고 있는 개인정보 보호법 제19조에 따라 차적자료를 다른 수사기관에 재제공할 수 없다고 보았다. 그럼에도 국가정보원 등

453) 다만 이때 테러 발생 시나 재해, 재난, 구급상황 발생 시는 제58조 제1항 제3호(공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보)에 해당한다고 보고 개인정보 보호법의 제3장부터 제7장까지의 적용을 함께 제외하였다.

국가안전보장과 관련된 범죄수사인 경우 제58조 제1항 제2호에 따라 제공할 수 있다고 보았다(개인정보 보호위원회 2018. 7. 9. 의결 제2018-15-146호).

결국 국가안전보장과 관련된 개인정보 처리에 대하여 현행 개인정보 보호법과 그 감독기관은 해당 처리가 법령상으로 특별한 규정이나 의무를 두고 있거나 소관 업무의 수행을 위하여 불가피한 경우인지 등을 전혀 살피지 않고 개인정보 보호법의 주요 적용을 포괄적으로 제외하고 있다.

유럽연합 GDPR의 경우 제23조에 제한 규정을 두고 국가안전보장(national security)을 지키기 위해 제5조, 제12조~제22조, 제34조에 규정된 의무 및 권리의 범위를 제한할 수 있도록 하였다. 다만 이는 유럽연합이나 회원국 법률의 입법 조치를 통해야 하고, 해당 조치의 규정이 제12조~제22조에 규정된 의무 및 권리에 상응해야 하며, 그러한 제한이 기본권과 자유의 본질을 존중할 뿐 아니라, 해당 조치가 민주 사회에서 필요하고 비례적인 조치인 경우에 한한다(GDPR 제23조제1항제(a)호). 이 때 위 입법 조치는 적절한 경우 최소한 (a) 처리 또는 처리 범주의 목적 (b) 개인정보의 범주 (c) 도입되는 제한의 범위 (d) 남용이나 불법 접근 또는 전송을 방지하기 위한 보호조치 (e) 컨트롤러 또는 컨트롤러 범주에 대한 상세설명 (f) 처리 또는 처리 범주의 성격, 범위 및 목적을 고려한 보관기간과 적용 가능한 보호조치 (g) 정보 주체의 권리와 자유에 대한 위험 (h) 제한에 대한 고지를 받을 정보 주체의 권리(단, 고지가 제한의 목적에 해를 미칠 수 있는 경우는 제외)에 관한 구체적 규정을 포함해야 한다(GDPR 제23조제2항).

한편 유럽평의회는 회원국과 개인정보 보호 협약 조인국들의 국가안전보장 관련 활동에도 유럽인권협약 제8조(사생활 및 가족생활을 존중받을 권리)를 적용하도록 하고 있다. 또 유럽인권재판소는 국가안전보장 관련 법률과 실무에서 이루어진 국가정보기관의 개인정보 처리 대해서도 협약 위반 여부를 판단해 왔다[454]. 예를 들어 유럽인권재판소는 2000년 루마니아법이 국가안전보장 관련 정보를 비밀파일에 수집, 기록 및 보관하도록 하면서 기관의 재량권 행사를 제한하지 않은 것이 유럽인권협약 제8조 위반이라고 결정하였다. 특히 국가 감시 조치의 대상이 되는 정보의 유형, 감시 대상이 되는 사람들의 범주, 감시 조치가 취해질 수 있는 상황 또는 절차를 규정하지 않은 것이 문제가 되었다[455]. 또 유럽인권재판소는 2006년 스웨덴 자유주의 정당과 공산주의 정당에 가입한 청

454) FRA(2018a), op. cit., p23.

구인들의 정보가 보안경찰기록에 장기간 보관된 것이 유럽인권협약 제8조 위반이라고 결정하였다. 재판소는 문제의 정보 보관에 법적 근거가 있으며 정당한 목적을 추구하였음을 인정하였으나, 1969년 집회에 대한 정보를 지금까지 보관한 것은 적절한 국가안보 이익을 추구한다고 할 수 없다고 보았다[455][456].

결국 국가안전보장과 관련한 개인정보의 예외에 대한 우리와 유럽의 개인정보 보호 체계를 비교하여 보았을 때, 국내 개인정보 보호법에서 제외되는 '국가안전보장'의 목적이 구체적이지 않고 제외 대상 개인정보의 항목과 기간이 모호하다는 문제가 두드러진다. 국가안전보장의 목적으로 개인정보 보호법의 적용을 제외하더라도 별도의 법률에서 그 제외 대상 개인정보의 수집·이용의 목적, 개인정보의 항목, 조치 업무 및 그 대상자의 범위, 안전성 확보 조치, 개인정보처리자의 명시, 개인정보의 보유 및 이용 기간, 정보주체에 대한 고지와 권리 행사 및 예외 등에 관한 구체적 규정을 포함해야 할 것이다. 특히 2013년 이후 유엔에서 국가의 통신 감시, 감청 및 개인정보 수집에 대해 적절한 투명성과 책무성을 보장할 수 있는 독립적이고 효과적인 국내 감독 체계를 설립하거나 운영할 것을 각국에 요청해 온 점을 고려하였을 때, 국가안전보장과 관련한 개인정보 처리에 대해서도 반드시 독립적이고 효과적인 감독 체계가 마련되어야 한다.

다. 범죄의 수사 및 형의 집행 관련 개인정보 처리의 광범위한 예외

앞서 제6장에서 살펴보았듯이 현행 개인정보 보호법은 범죄수사 및 형집행과 관련한 개인정보 처리에 대해서 많은 예외 규정을 두고 있으며, 이에 수반하는 감독 또한 미흡하게 이루어지고 있다.

우선 현행 개인정보 보호법은 제18조 제2항에서 공공기관이 보유한 개인정보에 대하여 수사기관이 범죄수사를 위해서 필요로 하는 경우나 구금시설이 형(刑) 및 감호, 보호처분의 집행을 위하여 필요로 하는 경우 특별한 요건이나 절차 없이도 목적 외로 제공

455) ECtHR(2020), Rotaru v. Romania [GC], No. 28341/95, para. 57; see also ECtHR(2007), Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, No. 62540/00; ECtHR(2011), Shimovolos v. Russia, No. 30194/09; ECtHR(2005), Vetter v. France, No. 59842/00.

456) ECtHR(2006), Segerstedt-Wiberg and Others v. Sweden, No. 62332/00, paras. 89 and 90; see also, for example: ECtHR(2013), M.K. v. France, No.19522/09.

하도록 하였으며, 이러한 제공 및 처리 대상에 민감정보와 고유식별정보도 광범위하게 포함되어 있다.

범죄수사 및 형집행 등과 관련된 개인정보파일의 경우 감독기관에 대한 등록 및 공개가 면제되어 있고 개인정보 처리방침도 수립 및 공개 의무가 없어 개인정보 보호 감독에서 전면적으로 제외되어 있다. 정보주체의 열람 및 정정·삭제권과 처리정지권의 행사, 정보주체의 고지받을 권리 역시 동반하여 제한되어 있어 정보주체의 권리 침해에 대한 인지와 권리구제가 상당히 어려운 상황이다.

또한 경찰은 구체적인 법령적 근거에 의하지 않고 상당히 방대한 개인정보 처리 시스템을 구축·운영해 왔다.

이처럼 현행 개인정보 보호법에 따라 범죄의 수사 및 형의 집행 관련 개인정보 처리에 대하여 감독하는 데에는 광범위한 예외와 한계를 노정하고 있다. 궁극적으로는 이를 보완하여 유럽연합 경찰 디렉티브 등 국제규범에 부응하는 입법적인 개선이 이루어져야 하겠지만, 법률 개정이 단기간 내 이루어지기 어려울 뿐더러 국가안전보장 및 범죄수사와 관련한 기관의 업무를 개인정보 보호법의 규율 대상에 입법적으로 포함할 수 있을지 장담하기 어려운 것이 사실이다. 그러나 국제 규범의 발전은 법집행 목적 개인정보 처리에 대해서도 원칙적으로 개인정보 보호 및 독립적인 감독 하에 포함시켜 왔다. 무엇보다 이 분야 정보주체의 권리구제를 방대한 예외 상황 속에 방치할 수 없는 상황임을 고려하여 볼 때, 현행 제도 속에서 국가인권기구의 기능을 통해 가능한 감독 방안을 모색해 볼 필요가 있다.

우리 국가인권위원회의 경우 경찰 등 수사기관이나 구금시설의 개인정보 처리에서 발생하는 정보인권 침해 문제에 대하여 진정 사건 처리와 조사의 권한을 행사할 수 있다. 따라서 국가인권위원회가 침해 조사 및 구제의 주요 대상인 구금·보호시설 및 수사기관의 개인정보 침해 사건에 대한 조사 및 구제 활동을 보다 강화한다면, 현행 개인정보 보호법에서 광범위하게 제외되고 있는 범죄수사 및 형집행 관련 개인정보 처리에 대한 권리구제가 보완될 수 있을 것이다. 국가인권기구로서 국가인권위원회가 고유의 조사 및 권고의 기능을 발휘하여 범죄수사 등을 목적으로 하는 개인정보 처리에 대하여 일정한 수준의 감독권을 행사하는 것이 가능하고 또 필요하다 할 것이다.

제2절 인권기구의 개인정보 보호 활동

이하에서는 국가인권기구의 개인정보 보호 업무에 관하여 살펴본다. 먼저 유럽 기본권청을 중심으로 해외 인권기구의 개인정보 보호 활동 사례를 검토하면서 개인정보 보호 감독기관과의 상호작용을 살펴본다. 이후 우리 국가인권위원회의 활동 사례를 짚어보고 시사점을 도출한다.

1. 인권기구와 개인정보 보호 감독기관의 상호작용

가. 유럽 기본권 옹호 체계와 개인정보 보호 감독

유럽연합 인권기구인 기본권청(FRA)은 개인정보 보호 감독기관, 평등기구, 국가인권기구를 3대 기본권 아키텍쳐[457](the fundamental rights architecture)로 지칭하며 이들 기본권 옹호기구들의 밀접한 협력 속에 인권 증진의 시너지 효과를 추구해야 한다고 보았다[458].

기본권청은 특히 2010년 <유럽연합의 개인정보 보호: 국가 개인정보 보호 감독기관의 역할>에 대한 보고서[459]를 발간하여 기본권 옹호기구로서 개인정보 보호 감독기관을 검토하였다. 이 보고서는 개인정보 보호 감독기관, 평등기구, 국가인권기구 등 유럽연합 3대 기본권 아키텍쳐와 관련한 이슈를 살펴본 기본권청의 <유럽연합의 기본권 아키텍쳐 강화 방안> 4개 보고서 중 하나이다. 기본권청은 이 3대 기본권 감독기관이 매우 상호관련성이 높고 유럽연합 기본권 아키텍쳐의 기반을 형성하고 있다고 보았다. 기본권청 역시 개인정보 보호 감독기관을 비롯하여 회원국내 기본권 분야 정부기관 및 공공기관과 협력할 수 있는 권한을 부여받았는데, 이는 국내적·지역적·국제적 차원에서 보다 효율

457) 정책 아키텍쳐는 정책의 여러 요소가 복잡하게 결합된 제도적 배열 구조를 말하며, 정책 아키텍쳐 혁신은 정책의 요소나 개념은 변화하지 않되 정책의 제도적 배열과 정책 요소간의 연계를 통해 혁신을 추구하는 의미로 사용되고 있음. 과학기술정책연구원(2006), 참여정부의 새로운 시도 : 정책 아키텍쳐 혁신 참조.

458) European Union Agency for Fundamental Rights(FRA) 의 Data Protection in the European Union: the role of National Data Protection Authorities: Strengthening the fundamental rights architecture in the EU 시리즈 참조.

459) FRA(2010b), op. cit.

적으로 기본권을 보호하고 증진하기 위한 필요성에서 기인한 것이다.

이 보고서에서 기본권청은 유럽연합 각 회원국의 개인정보 보호 감독기관 현황을 살펴보고 독립성이 취약하다는 문제점을 발견하였다. 향후 감독기관의 취약한 독립성을 보완하기 위한 방안으로 기본권청은 국가인권기구에 대한 '파리 원칙'을 참고하여 개인정보 보호 디렉티브를 개선할 것을 권고하였다. 또 기본권청은 개인정보 보호 감독기관이 국가인권기구 및 평등기구 등 여타의 기본권 보호기구들과 밀접한 협력과 시너지를 증진해야 한다고 보고, 개인정보 보호 감독기관을 국가인권 체제의 특수 분야로 포함할 것을 제언하기도 하였다[460].

한편, Peter J. Hustinx 유럽 개인정보 보호 감독관(European Data Protection Supervisor, EDPS)은 2013년 유럽연합 GDPR 제정을 앞두고 개인정보 보호 감독기관과 국가인권기구 간의 협력 및 업무 관련성에 대하여 검토하였다[461].

Hustinx는 국제적인 규범에 따라 설립된 개인정보 감독기관과 국가인권기구들의 상호작용이 향후 점차 일치되고 예측 가능한 형태를 띨 것이라고 보았다. 개인정보 감독기관은 완전한 독립성과 외부 영향 회피 원칙 하에 구속되지만 이러한 원칙이 두 기관 간 협력을 제지하지는 않을 것이라고 한다. "사법기관 및 (특히 옴브즈만과 중재인 및 유사기관과 같이) 그밖에 인권의 보호 및 향상에 책임 있는 기관들과 지속적으로 협의해야 한다." 고 규정한 파리 원칙에 따라 독립적인 국가인권기구 역시 비슷한 기준이 적용될 것이다. 공통의 관심사를 위한 상호관계를 어떻게 발전시키고 관련 체계를 수립할 것인가의 문제는 양 당사자 기관에 달렸다.

국가 평등기구나 국가 옴부즈만의 경우에서와 마찬가지로 많은 국가에서 개인정보 감독기관은 국가인권기구의 주요 이해관계자 중 하나로서, 인권 의제에 적극적으로 기여할 수 있다. 개인정보 감독기관과 국가인권기구 간의 상호작용이 가장 활발한 영역은 공식적인 권한 및 절차에 대한 의존도가 낮은 인식 제고와 교육 분야에서의 협력으로 볼 수 있다. 소관 및 처리 절차가 법률로 규정된 진정 사건 처리와 조사의 경우 기관 간에 활발한 상호작용이 어려울 수도 있지만, 개인정보 감독기관의 진정이나 조사 대상이 될 수

460) 이때 Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin 가 평등기구에 대한 규정(제13조)에서 국내 인권기구의 일부로서 평등기구를 규정하였다는 사례를 들고 있다.
461) Peter J. Hustinx(2013), op. cit., pp157-172.

있는 구조적 문제나 특수 영역의 문제를 드러내는 데 국가인권기구가 유용한 역할을 수행할 수 있으며, 때로는 직접 진정의 개시자 역할을 할 수도 있다.

GDPR에 따르면 "정보주체는, 회원국 법률에 따라 적절하게 구성되고 공익을 위한 법정 목표를 가지며 개인정보 보호와 관련한 정보주체의 권리 및 자유 보호 분야에서 활동하고 있는 비영리단체, 기관 또는 협회에 대하여, 정보 주체를 대신해서 개인정보 보호 감독기관에 진정을 제기하고, 정보주체를 대신해서 권리를 행사하고, 회원국 법률에 규정된 경우 정보 주체를 대신해서 보상을 받을 권리를 행사하도록 위임할 권리가 있다(제80조)." 이 규정은 유럽연합 회원국 내에서 정보주체를 대리하거나 진정사건을 처리하는 다른 국가기관들이 정보주체의 권리를 보호하기 위하여 협력하는 범위를 확대하는 근거가 될 수 있다. 다만 각국에서 국가인권기구가 지금까지 보다 어느 정도까지 개인정보 보호 문제에 직접 관여할 수 있을지에 대한 구체적 사례는 좀 더 지켜볼 필요가 있다.

나. 유럽연합 기본권청의 개인정보 보호 업무

유럽연합 기본권청은, "유럽연합 법을 실시함에 있어 유럽연합 제 기관과 부속기구 및 회원국이 기본권에 관한 조치와 행동을 채택할 때 기본권이 충분하게 보장될 수 있도록 그에 관한 지원과 전문지식을 제공할 목적"으로 설립된 기본권 전문기구이며, '파리 원칙'(Paris Principles), 즉 유엔이 마련한 '독립적 국내인권기구'의 설립에 관한 표준 모델에 따랐다.

기본권청의 주된 역할은 기본권 보호를 책임지고 있는 관련 기구들과의 대화와 협력 네트워크의 구축이다. 기본권청은 회원국의 국내인권기구뿐 아니라 유럽 및 국제적 차원의 다양한 기구, 이를테면, 유럽평의회, 유럽안보협력기구(OSCE), 유엔 및 기타 국제기구들과 긴밀한 대화와 협력 관계를 유지하고 있다. 다만 기본권청이 주로 기본권에 관한 정보의 보급 혹은 확산이라는 역할을 맡고 있는 관계로 인권침해에 대한 조사 및 구제조치를 취할 수 있는 권한은 가지고 있지 않고, 기본권청이 택한 결론, 견해 및 보고는 권고적 효력만 가지고 있을 뿐 법적 구속력 있는 행위로는 작용하지 않는다[462].

462) 채형복(2013). EU 기본권청, 동아법학 58, p123-161.

2007년 설립된 기본권청은 설립 이후로부터 유럽 개인정보 보호와 관련한 주요한 정책에 대하여 의견을 내고 정책적으로 개입해 왔다. 이는 기본권청이 유럽 기본권헌장의 사생활권과 개인정보 보호권을 기본적으로 소관하고 있기 때문이기도 하지만, 기본권청의 법적 임무인 "특수주제에 관한 결론 및 견해의 공표" 대상에 "정보 사회, 특히 사생활 및 개인정보 보호 문제"가 포함되어 온 데 기반한 것이다. 기본권청의 특수주제(thematic areas)는 유럽의회 논의를 거쳐 유럽 이사회가 채택하는 5개년 프레임워크(five-year Multiannual Framework)를 통해 정해지는데, 설립 이후 여기에 "정보 사회, 특히 사생활 및 개인정보 보호 문제" 문제가 줄곧 포함되어 왔다[463]. 최근 기본권청은 "개인정보 보호, 프라이버시 및 신기술"에 대한 업무에서 △인공지능 및 빅데이터 문제, △국경과 정보 시스템 문제, △개인정보 보호, △불법적 프로파일링의 세부 주제를 두고 분야별 의견을 제시하고 있다.

유럽연합은 개인정보 보호 감독기관으로 유럽 개인정보 보호 감독관(European Data Protection Supervisor, EDPS)을 두고 개인정보 보호 디렉티브에 따른 전문 자문기구로 제29조 작업반(Article 29 Working Party)[464]을 두어 왔지만, 기본권청은 EDPS 및 제29조 작업반과 별도로 독자적인 의견을 발표해 왔다. 예를 들어 2011년에 유럽연합 집행위원회가 테러 방지 등을 위한 승객예약자료(PNR: Passenger Name Records) 이용 디렉티브안을 마련하자 EDPS[465]와 제29조 작업반[466]은 물론, 기본권청[467]도 독자적인 의견을 발

463) 기본권청의 <2018-2022 다년 프레임워크(Multi-annual Framework 2018-2022)>에서는 특수주제에 대한 업무 영역은 다음과 같다. a. 범죄 피해자 및 사법접근권 문제 b. 평등 및 차별 문제 c. 정보 사회, 특히 사생활 및 개인정보 보호 문제 d. 형사상 문제를 제외한 사법협력 문제 e. 난민과 이주민의 이민, 출입국, 망명 및 사회 통합 문제 f. 인종차별, 외국인 혐오증 및 관련 편협함의 문제 g. 아동의 권리 h. 롬인의 사회통합 및 사회적 포용.

464) 2016년 GDPR 제정 이후 유럽정보보호위원회(European Data Protection Board, EDPB)로 대체되었음.

465) EDPS(2011), Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

466) ARTICLE 29 DATA PROTECTION WORKING PARTY(2011), Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

467) European Union Agency for Fundamental Rights(FRA)(2011), FRA opinion on the proposal for a Passenger Name Record (PNR) Directive.

표하였다. 유럽의회가 2011년 보안 스캐너에 특별히 초점을 맞춘 항공 보안 결의안을 마련할 때에도 EDPS, 제29조 작업반, 기본권청의 자문을 모두 받았다[468].

2012년에는 유럽연합의 개인정보 보호 개혁 패키지, 즉 GDPR과 경찰 디렉티브 제정안에 대하여 EDPS[469]와 기본권청[470]이 각각 그에 대한 의견을 냈다. 특히 기본권청은 유럽연합 개인정보 보호 개혁 과정에서 적극적인 조언자 역할을 수행하였다. 2013년 기본권청은 유럽연합 16개국 개인정보 보호 감독기관 및 700명을 직접 인터뷰하여 개인정보 보호 법제도 및 감독 체계에 대한 개선 의견을 담은 보고서를 발표하였다[471]. 이 보고서는 개인정보 권리 보호의 핵심 역할자(key players)인 유럽 각국 국가 개인정보 보호 감독기관들이 적절한 자원과 권한 행사에서 부족한 면이 있다고 진단하며, 정보주체 권리 구제를 위하여 유럽연합이 개인정보 보호 개혁 입법에서 개인정보 보호 감독기관의 실효성을 제고할 것을 요구하였다. 즉 각국 개인정보 보호 감독기관의 독립성을 강화하고 권한과 소관을 확충하며 재정적, 인적 자원을 적절히 지원받아 법적, 기술적으로 다양하고 전문적인 역량을 확보해야 한다는 것이다. 또 권리구제가 실효적이려면 시민사회단체 및 법원의 역할도 강화될 필요가 있다고 보았다. 기본권청은 이 보고서에서도 개인정보 보호 감독기관이 유럽연합 기본권 아키텍쳐의 일원으로서 다른 기본권 보호기구들과 좀 더 긴밀한 협력 및 시너지를 추구해야 한다고 강조하였다. 2014년에는 기본권청과 유럽평의회가 공동으로 유럽연합과 유럽평의회의 규범을 아우르는 개인정보 보호법 해설서를 발간하였다. 유럽 개인정보 보호 규범의 모범적이고 일관된 적용을 위한 해석을 담은 이 핸드북은 2018년에 개정판을 발간하면서 EDPS 및 유럽인권재판소와도 협력하였다[472].

개인정보 보호 관련 기본권청의 최근 활동으로는 다음과 같은 것을 들 수 있다. 기본권청은 2018년 5월 정보기관의 감시 문제를 기본권 보호와 권리구제 측면에서 살펴본

468) Official Journal of the European Union, 2013.2.5., “C 33 E/125”, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011IP0329&from=EN>.
469) EDPS(2012), Opinion of the European Data Protection Supervisor on the data protection reform package.
470) European Union Agency for Fundamental Rights(FRA)(2012). Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package.
471) European Union Agency for Fundamental Rights(FRA)(2013), Access to data protection remedies in EU Member States.
472) FRA(2018a), op. cit.

보고서를 발간하였고[473], 2018년 9월에는 “신분증명서류 및 주민등록증에서 생체인식정보 보관이 기본권에 미치는 함의”에 대한 의견을 발표하면서 이 분야 EDPS의 의견을 보완한다고 밝혔다[474].

또한 2018년 발표된 “빅데이터, 알고리즘 및 차별”에 대한 보고서[475]를 필두로 신기술 분야 사생활 및 개인정보 보호 문제를 주목하는 후속 연구 및 자료 발표가 계속되었다. 2018년 12월 발간된 “현재와 장래의 불법 프로파일링 방지를 위한 가이드”는 특히 법집행 및 출입국 관리 분야 공무원 교육을 염두에 두고 제작되었으며, GDPR 및 경찰 디렉티브에 규정된 개인정보 프로파일링과 관련된 주요 법적 요건을 정리하였다[476]. 2019년에는 유럽에서 논란이 커지고 있는 법집행 기관의 얼굴인식 기술의 기본권 제한에 대한 보고서를 발간하였다[477].

GDPR의 준수 및 감독과 직접 관련한 활동도 계속하고 있다. 기본권청은 2019년 7월 12일 GDPR 시행 1년 보고서를 발간하였다. GDPR과 시민사회에 초점을 맞춘 이 보고서는 개인정보 보호 요건에 대한 시민사회의 이해도, 시민사회의 준수 문제, 감독기관과의 상호작용, 이행 노력, GDPR 진정 경험 등을 정리하고 유럽 집행위원회의 공식 GDPR 영향 평가에 통찰력을 제공하고자 하였다[478]. 2020년 6월에는 유럽 전역에서 시민 35,000명을 대상으로 “개인정보와 프라이버시권”에 대한 인식 조사를 실시하고 그 결과를 발표하였다[479].

한편 최근 코로나19 위기가 확산되자 기본권청은 그에 대한 대응에서 개인정보 보호권 및 인권적 접근을 강조하는 자료 및 의견을 발표하고 있다[480].

---

473) European Union Agency for Fundamental Rights(FRA)(2018b), Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union - Volume II - Summary.
474) European Union Agency for Fundamental Rights(FRA)(2018c). Fundamental rights implications of storing biometric data in identity documents and residence cards.
475) European Union Agency for Fundamental Rights(FRA)(2018d), In Brief - Big data, algorithms and discrimination.
476) European Union Agency for Fundamental Rights(FRA)(2018e), Preventing unlawful profiling today and in the future: a guide.
477) European Union Agency for Fundamental Rights(FRA)(2019a), Facial recognition technology: fundamental rights considerations in the context of law enforcement.
478) European Union Agency for Fundamental Rights(FRA)(2019b), The General Data Protection Regulation - one year on.
479) European Union Agency for Fundamental Rights(FRA)(2020a), Your rights matter: Data protection and privacy - Fundamental Rights Survey.

다. 코로나19 위기에서 인권기구와 개인정보 보호 감독기관의 협력

국제적으로 인권기구와 개인정보 보호 감독기관은 개인정보 보호 및 정보인권 침해 우려에 대하여 직간접적으로 협력해 왔다. 특히 최근 코로나19의 지구적 확산 속에 인권기구와 개인정보 보호 감독기관 간 협력과 상호작용 노력이 눈에 띈다.

우리나라 국가인권위원회 위원장 성명서를 통해 확인한 바대로[481], 코로나19 감염병 위기에 대응하기 위해 취해진 민관의 다양한 조치들은 사생활권과 개인정보 보호권 등 기본권에 중대한 영향을 미친다. 세계 여러 나라에서 방역을 이유로 감염인 추적과 감시 정책을 추진하면서 정보인권의 위기 또한 고조되었고, 각국 또는 지역 인권기구와 개인정보 보호 감독기관이 이에 대응하는 과정에서 때로 적극적으로 협력하는 모습을 보이고 있다.

유럽 기본권청과 EDPS는 2020년 6월 감염병 위기 상황에서 유럽연합 전역에 걸쳐 개인정보 보호 문제에 협력하고 인권을 보호하기 위해 양해각서를 갱신하였다. 두 기관은 이미 2017년에 관련 분야에서 공통의 이해관계를 인정하고 더 많은 협력을 할 수 있도록 한 차례 양해각서를 체결한 바 있다. 이번 양해각서를 갱신하면서 두 기관은 유럽연합 국가들이 새로운 코로나바이러스 접촉자 추적앱을 계속 도입하고 있는 상황을 언급하면서 "프라이버시와 개인정보 보호 등 기본권에 대한 존중이 숙고 대상이 되어야 한다"는 공동의 입장을 표명했다[482]. 보도자료에서 Michael O'Flaherty 기본권청장은 "기술은 사람들의 기본권과 개인정보 보호 원칙을 존중하면서 올바르게 사용되어야 한다. EDPS와의 새로운 협력은 우리가 중요한 이 문제를 강조하고 유럽에서의 권리 존중 관행을 촉진하는 데 도움이 될 것이다."고 강조하였다. Wojciech Wiewiórowski 감독관은

480) European Union Agency for Fundamental Rights(FRA)(2020b), "Fundamental rights implications of COVID-19", <https://fra.europa.eu/en/themes/covid-19>.

481) 국가인권위원회, 2020.3.9., "과도한 동선 공개로 인한 사생활 침해 위원장 성명서"; 국가인권위원회, 2020.4.9.. "손목밴드 도입 논의 등 과도한 자유권 훼손에 대한 위원장 성명서".

482) European Union Agency for Fundamental Rights(FRA)(2020c), EU rights and data protection bodies: new technology and data protection have to go hand in hand, 2020.6.22., <https://fra.europa.eu/en/news/2020/eu-rights-and-data-protection-bodies-new-technology-and-data-protection-have-go-hand-hand?pk_campaign=FRA-Alerts-Newsletter&pk_source=newsletter>.

EDPS로서 유럽연합 내 개인정보 보호에 대한 기본권이 존중되도록 할 책임이 있고, 이를 위해 기본권청을 비롯한 다른 유럽연합 기구와 협력한다고 밝혔다. 기본권청과 EDPS는 앞으로도 개인정보 문제를 집중 조명하기 위해 협력할 계획이다.

유럽 개인정보 보호 감독관(EDPS)과 유럽연합 기본권청(FRA) 간
협력 증대에 관한 양해각서 갱신[483)]

2020. 6. 22.

I. 서문

1. 본 문서는 다음 기구들 간의 협력 증진 원칙을 정하는 양해각서이다.
Regulation (EU) 2018/1725 of the European Parliament and of the Council 에 의해 설립된 EDPS와 그 감독관으로서 이 기구를 대표하여 양해각서에 서명하는 Wojciech Wiewi6rowski 및 Council Regulation (EC) No. 168/2007 에 의해 설립된 FRA와 그 청장으로서 이 기구를 대표하여 양해각서에 서명하는 Michael O'Flaherty.
2. EU 규정 2018/1725 제52조에 따라, EDPS는 EU 기관 및 기구의 개인정보의 처리에 있어 자연인의 기본권과 자유, 특히 그 개인정보 보호권이 존중받도록 책임지는 독립 감독기관이다.
3. EC 규정 No. 168/2007 제2조에 따라, FRA는 유럽연합 및 그 회원국의 관련 기관, 기구, 사무소 및 공공기관들이 유럽연합 법을 시행함에 있어 각 기관이 소관 내에서 조치를 취하거나 행동 방침을 수립할 때 기본권을 완전히 존중하도록 지원하기 위해 기본권과 관련한 지원과 전문지식을 제공할 책임이 있다.
4. EU 결정 2017/2269 제2조제c항에 따라, FRA는 EDPS의 책임 권한에 대한 침해 없이 정보사회, 특히 사생활권 및 개인정보 보호 보장에 관한 업무를 수행하도록 되어 있다. EC 규정 No 168/2007 제7조에 따라, FRA는 관련 유럽연합 기구, 사무실 및 기관들과 적절하게 협력할 책임이 있다. EU 결정 2017/2269 전문6에 따라, FRA의 업무와 다른 유럽연합 기관, 특히 EDPS의 업무 간에 상호보완성이 보장되어야 한다.

II. 목적

5. 본 양해각서는 EDPS와 FRA의 공통 관심사를 인정하여 관련 분야에서 보다 협력하기로 합의하였다. 양해각서는 이전의 교류에 기초하여 유럽연합 법에 따른 각자의 법적 의무와 합치되게 그 한도 내에서 협력관계를 수립, 정의, 장려 및 개선하는 것을 목표로 한다.
6. 본 양해각서는 유럽연합 기구인 FRA의 개인정보 처리에 대한 감독기관으로서 EDPS의 의무와 권한에 영향을 미치지 않으며, EU 규정 2018/1725에 따른 개인정보 컨트롤러(data controller) 또는 개인정보 프로세서(data processor)로서, 또한 (EC) 규정 No 168/2007에 따른

독립 전문기구로서 FRA의 의무에 어떠한 영향도 미치지 않는다.

Ⅲ. 연락 및 정보 교환

7. FRA와 EDPS는 특히 본 양해각서의 조항과 관련하여 정기적으로 협력 조정 및 상호 협의를 담당하는 단일연락창구를 수립하는 것에 합의한다.

8. FRA와 EDPS는 연락창구에 대한 세부사항을 교환하고 연락창구에 관한 변경사항을 서면 지체 없이 서로 통보하기로 합의한다.

9. FRA와 EDPS는 컨퍼런스, 결의안, 실무단(working group) 등 다양한 장에서 협력 분야로 확인된 계획들에 대한 정보를 공유하기로 합의한다.

10. FRA와 EDPS는 최소 1년에 한 번 만나 공통의 전략적 관심사를 검토하고, 협력 분야를 파악하며, 프라이버시, 개인정보 보호 및 관련 권리 등 기본권에 대한 주요 당면 과제에 대한 의견을 교환하는 것을 목표로 한다.

11. FRA와 EDPS는 본 양해각서에서 확인된 협력 분야와 관련이 있는 한 업무 프로그램 및 실행 계획과 같은 전략 문서를 작성하는 과정에서 서로 정보를 제공하고 의견을 교환하는 데 합의한다.

Ⅳ. 연구 및 의견

12. FRA와 EDPS는 상호 관심사의 향후 연구 활동에 대한 정보를 교환하고 공통의 전략적 이해관계에 대한 당해 의견을 교환하기로 합의한다.

13. FRA와 EDPS는 서로 관련 전문가 회의에 초청하고 적절한 경우 연구 활동에 협력하기로 합의한다.

14. FRA와 EDPS는 협력 분야와 관련된 정보와 데이터의 수집, 기록 및 분석에 협력하기로 합의한다.

15. FRA와 EDPS는 공통 관심 분야와 관련된 공동 훈련 활동을 조직하고 다른 기관이 조직하는 훈련 활동에 공동으로 기여하는 것을 고려하기로 합의한다.

Ⅴ. 비용 및 조달

16. 사례별로 달리 합의되지 않는 한, 본 양해각서를 이행하는 과정에서 발생할 수 있는 자체 비용을 FRA와 EDPS가 각각 부담한다.

17. 본 양해각서에 명시된 협력 목표를 달성하기 위해, FRA와 EDPS는 적절한 경우 공동 조달을 실시하거나 상대방이 비용보전을 위해 단일 조달 실시를 허용하는 것을 고려하기로 합의한다.

Ⅵ. 기밀 유지

18. FRA와 EDPS는 정보, 문서 또는 기타 서로 교류한 자료를 각각 기밀로 유지하고, 공개 당

사자의 사전 서면 동의 없이는 그러한 기밀 자료를 공개하지 않는다.

19. FRA와 EDPS는 양해각서의 목적상, EU RESTRICTED/RESTREINT UE 이상의 유럽연합 기밀 정보는 당사자들 간에 교환될 수 없다는 점에 합의한다. 그들은 유럽연합 기밀 정보의 보호와 관련된 모든 보안 조치를 준수하는 것에 합의한다.

VII. 발효 및 갱신

20. 본 갱신 양해각서는 FRA와 EDPS가 서명한 다음 날부터 시행되며, 2017년 3월 30일에 서명한 FRA와 EDPS 간의 양해각서를 대체한다.

21. FRA와 EDPS는 언제든지 상호 동의하에 본 양해각서를 수정하거나 보완할 수 있다. 이러한 수정사항, 보충사항 또는 종료사항은 서면으로 작성한다.

22. FRA와 EDPS는 본 양해각서에 따라 정기적인 협력을 검토하기로 합의한다. (끝)

한편, 프랑스의 경우 블루투스 기반 접촉자 추적앱 'StopCovid'에 대한 정부 법안이 발표되자, 개인정보 보호 감독기관과 국가인권기구는 물론 여러 관련 기관들이 이에 대한 의견을 발표하였다. 이러한 노력들은 이 앱과 관련 법안이 인권 및 개인정보 보호 관련법을 준수하도록 압력을 발휘한 것으로 평가받는다[484]. 다만 개인정보 보호 감독기관인 CNIL과 국가인권기구인 CNCDH는 각 의견에서 다소 차이를 드러냈다. CNIL의 경우 GDPR 원칙에 따른 앱의 이용조건을 제시하면서, 가명정보 사용, GPS 사용금지, 감염자에 대한 개인정보파일 생성 금지, 자율적 사용 등을 요구하였으며, 정기적인 개인정보보호 영향평가에 따라 계속 시행 여부를 결정하는 조건부 실시를 제안하였다. 반면 CNCDH의 경우, GDPR 준수만으로는 기본권을 보호하기에 충분치 않다고 지적하면서 이 앱의 효과가 불분명하고 기본권 간섭이 비례적이지 않다고 우려를 표했다. 두 기관 간 이러한 견해 차이는 현행 개인정보 보호법의 준수 여부를 중심으로 판단하는 개인정보 보호 감독기관과, 국제인권규범 및 헌법에 의거해 필요성과 비례성을 판단하는 인권기구 간 역할 차이로 인한 것으로 보인다.

---

483) EDPS, "Revised Memorandum of Understanding on increasing cooperation between the European Data Protection Supervisor and the European Union Agency for Fundamental Rights", <https://fra.europa.eu/sites/default/files/fra_uploads/mou_edps-fra_revised_signed.pdf>.

484) WLG, 2020.5.31., "France: COVID-19 and the "StopCovid" App", <https://www.theworldlawgroup.com/news/covid-19-and-the-stopcovid-app>.

영국에서는 ‘코로나19 접촉자 추적앱’에 대한 정부 법안에 대하여 2020년 5월 스코틀랜드 인권위원회와 국회 인권상임위원회, 개인정보 보호 감독기관이 각각 우려의 목소리를 냈다. 영국 개인정보 보호 감독기관인 ICO는 <코로나19 접촉자 추적: 앱 개발에 있어 개인정보 보호에 대한 기대> 의견을 발표하고 이 앱의 목적, 대상, 범위, 개인정보 보호법 준수 사항 및 원칙을 제시하였다[485]. 스코틀랜드 인권위원회는 접촉자 추적앱이 사생활에 대한 중대한 간섭을 야기하므로 1차 입법(Primary legislation)으로 의회에서 제정되어야 하며, 독립적인 감독을 받아야 하고, 평등과 비차별 원칙을 준수해야 한다고 지적하였다[486]. 국회 인권기구에 준하는 상하원 공동 인권상임위원회 역시 접촉자 추정앱 법안의 프라이버시 및 개인정보 보호 문제에 대한 우려를 표하였다. 위원회는 특히 ‘디지털 접촉자 추적 인권 감독관’(digital contact tracing human rights commissioner)의 신설과 감독을 요구하면서, 이 감독관이 ▲ 접촉자 추적앱에서 프라이버시, 개인정보 보호, 인권 관련 법의 적용 문제 ▲ 정부부처 및 공공기관 정보 처리 시스템의 보안 문제 ▲ 개인 식별의 위험성 ▲ 디지털 접촉자 추적이 필요적이고 비례적인지 여부 등을 검토하며 ▲ 진정 및 구제 절차도 담당하도록 하였다[487]. 인권기구들의 의견에서는 공통적으로 감염병 위기에 대응할 수 있는 독립적인 인권 감독 기능을 요청하고 있다는 점이 시사적이다.

485) ICO(2020), COVID-19 Contact tracing: data protection expectations on app development, <https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf>.

486) Scottish Human Rights Commission(2020), COVID - 19: Human Rights implications of digital contact tracing technology, <https://www.scottishhumanrights.com/media/2028/contact-tracing-briefing-180520-final.pdf>.

487) ComputerWeekly, 2020.5.12., "Draft Covid-19 contact tracing legislation proposes formal oversight", <https://www.computerweekly.com/news/252482995/Draft-Covid-19-contact-tracing-legislation-proposes-formal-oversight>.

라. 인공지능 등 신기술 환경과 인권기구의 역할

영국 세계디지털파트너와 미 스탠퍼드대학교 세계디지털정책인큐베이터는 2020년 4월 각국의 인공지능 국가 전략을 분석한 공동보고서에서 인공지능 국가전략에 인권을 통합할 것을 권고하였다[488]. 공동보고서에 따르면, 정부가 인권 존중 인공지능 정책의 기반을 다지기 위해 인공지능 국가전략에서 취할 수 있는 조치로 다음을 들 수 있다.

첫째, 인공지능 국가전략 전반에서 인권 원칙의 명시적 포함. 인공지능이 인권에 미치는 영향과 그 영향의 위험성을 완화시킬 방안을 고려하는 것이 인공지능 국가전략의 핵심이어야 한다. 각 분야들은 인권과 관련하여 인공지능이 유발하는 위험성과 가능성을 검토해야 하며, 위기 계층, 취약 계층, 소외 계층에 특별히 주목해야 한다. 둘째, 인권을 보호하는 구체적인 조치들의 개괄. 인공지능 국가전략을 인권과 연계하면서, 인권을 보호하기 위한 구체적인 목표, 책무 또는 실행 방안을 포함해야 한다. 셋째, 권리 존중 관행을 보장하기 위한 우대정책 또는 특별 요건 수립. 정부는 인공지능 국가전략에서 인권 보호 목표 달성 뿐 아니라 인권 존중 관행과 실행을 장려하기 위해 모든 분야에 걸친 조치를 포함해야 한다. 넷째, 인권 침해에 대한 불만처리 및 구체 절차 수립. 인공지능 국가전략은 인공지능 관련 인권 침해의 피해자가 이용할 수 있는 현행 불만처리 및 구제 절차를 살펴보고, 그 충분성 여부를 판단해야 한다. 인공지능 기술의 특수성에 따라 이러한 절차(법적 근거 포함)들을 개정하거나, 해당 절차에서 인공지능 관련 불만을 처리하는 담당자들의 역량 강화가 필요할 수 있다. 다섯째, 지역적, 국제적 차원의 인공지능 정책 인식. 인공지능 국가전략은 인공지능과 관련하여 지역적, 국제적 측면과 과정, 그리고 인권 존중 접근 방식과 성과를 촉진하기 위한 정부의 능동적인 참여 방안을 명확히 파악해야 한다. 여섯째, 인공지능 국가전략 초안 작성시 인권전문가 및 이해관계자 포함. 인공지능 국가전략 초안을 작성할 때, 정부는 인권 전문성과 인공지능이 인권에 미치는 영향이 작성 과정의 핵심이 되도록 보장해야 한다. 인권단체 뿐 아니라 인공지능으로부터 악영향을 받거나 특정 응용과정에서 혜택을 받을 수 있는 광범위한 시민사회단체 및 공동체를 대표하는 이해관계자들이 이 과정에 참여해야 한다.

488) Global Partners Digital, Global Digital Policy Incubator(2020), National Artificial Intelligence Strategies and Human Rights: A Review, <https://www.gp-digital.org/wp-content/uploads/2020/04/National-Artifical-Intelligence-Strategies-and-Human-Rights%E2%80%94A-Review_.pdf>.

공동보고서에 따르면 아쉽게도 한국은 인권 체계 대신 윤리적/사람중심 접근을 취한 국가로 분류된다. 스탠포드대학교-뉴욕대학교의 또 다른 2020년 2월 공동연구에 따르면 성능이나 알고리즘의 편향성을 방치할 경우 정부와 시민들 사이의 신뢰를 떨어뜨릴 우려가 있다[489]. 국민들에게 신뢰받는 인공지능 국가전략을 위해서는 차별금지 및 권리구제 등 인권적 접근을 보장할 필요가 있고, 여기서 국가인권기구의 적극적인 역할이 필요하다 할 것이다.

이러한 시대적 요청이 부응하여 최근 유엔 등 국제인권기구 및 각국 국가인권기구들은 인공지능에 대한 인권적 접근과 규제 체제 논의를 이끌고 있다. 유엔 의사표현의 자유 증진 및 보호를 위한 특별보고관(David Kaye)[490]과 인권최고대표실[491]은 2018년 <인공지능 기술과 표현의 자유>에 대한 보고서와 팩트시트에서 국제인권법에 기반한 인공지능 규제 체제를 다음과 같이 제안하였다.

첫째, 인권 원칙. 인공지능은 모든 다른 기술과 마찬가지로 국제인권법에 따른 국가의 의무와 민간기업의 책임을 준수하여 설계되고 개발되고 도입되어야 한다. 기업은 그 표준, 규정, 시스템 설계를 보편 인권 원칙에 맞추어야 한다. 둘째, 투명성. 인공지능 시스템은 개인에게 적극적으로 공개되어야 하며, 이들이 인공지능 절차에 자신의 데이터를 적용하거나 투여한다는 사실을 이해할 수 있는 방식으로 공개되어야 한다. 기업과 정부는 인공지능 가치 체계의 각 측면에 걸쳐 투명성을 수용해야 한다. 기업은 개인 이용자에게 인공지능 시스템의 존재 여부, 그 목적, 구성 및 영향에 대해 교육해야 한다. 기업

489) David Freeman Engstrom, Daniel E. Ho, Catherine M. Sharkey, Mariano-Florentino Cuéllar(2020), Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies, <https://law.stanford.edu/education/only-at-sls/law-policy-lab/practicums-2018-2019/administering-by-algorithm-artificial-intelligence-in-the-regulatory-state/acus-report-for-administering-by-algorithm-artificial-intelligence-in-the-regulatory-state/#slsnav-report>; VentureBeat(2020), “Stanford and NYU: Only 15% of AI federal agencies use is highly sophisticated”,2020.2.19. <https://venturebeat.com/2020/02/19/only-15-of-ai-federal-agencies-use-is-highly-sophisticated-according-to-stanford-and-nyu-report/>

490) David Kay(2018), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348.

491) OHCHR(2018), “Artificial Intelligence Technologies and Freedom of Expression: A human rights approach to Artificial Intelligence (AI)”, <https://www.ohchr.org/Documents/Issues/Expression/Factsheet_3.pdf>.

은 얼마나 많은 내용이 삭제되고, 얼마나 자주 삭제를 요청받는지, 얼마나 자주 삭제에 대한 이의가 제기되는지를 공개해야 한다. 셋째, 인권영향평가. 정부와 기업은 인공지능 시스템을 면밀히 조사하고 개념에서 구현에 이르기까지 이의를 제기할 수 있는 조치를 취해야 한다. 인권영향평가는 인공지능 시스템의 인권 영향 문제를 해결하기 위한 하나의 도구이다. 넷째, 감사. 인공지능 시스템의 외부적 검토를 촉진하는 것은 엄격하고 독립적으로 투명성을 보장하는 데 중요하다. 다섯째, 개인의 자율성. 인공지능이 개인의 의견 형성 및 보유 역량과 정보 환경에서 접근하고 표현하는 역량을 비가시적으로 대체하거나 조작하거나 방해해서는 안 된다. 개인의 자율성을 존중하는 것은 최소한 이용자가 지식, 선택 및 통제권을 갖도록 보장하는 것을 의미한다. 여섯째, 고지 및 동의. 기업은 플랫폼, 사이트 또는 서비스의 이용에 자사 인공지능이 어떻게 관여하고 있는지를 이용자에게 충분히 알려야 한다. 일곱째, 권리구제. 인공지능 시스템이 인권에 악영향을 미친다면 관련 기업이 이를 구제하는 것이 가능해야 하고 구제되어야 한다.

최근에는 인공지능 의사결정의 불투명성과 차별적 효과에 대한 우려가 커지고 있다. 그 일례로 미국 법원에서 피고인의 재범 위험성을 평가할 때 참고하는 콤파스(COMPAS) 알고리즘의 경우 흑인과 백인 피고인 간에 인종 편향성을 드러내어 논란을 빚었다[492]. 또한 영국에서는 교육부와 시험감독청장이 코로나19 확산으로 대학수학능력시험 A레벨을 취소하는 대신 인공지능으로 학생 성적을 부여하였는데 그 결과가 부유한 지역 학생과 가난한 지역 학생 간에 편향성을 드러내어 사회적으로 큰 논란을 빚었다[493]. 네덜란드의 사회복지 위험발견시스템(SyRI)은 중앙정부 및 지자체가 본래 분리 보관되어 있던 데이터들을 광범위하게 결합하여 이를 비공개 인공지능 "위험 모델"에 기반해 분석 후

492) 언론사 프로퍼블리카에서 2013년부터 2014년까지 콤파스 알고리즘에 의해 법원의 결정이 이루어진 피고인 1200명의 기록을 검증한 결과, 재범률이 높은 것으로 예측되었지만 실제로 2년간 범죄를 저지르지 않은 경우가 흑인의 경우 45%, 백인의 경우는 23.5%이었던 반면, 재범률이 낮은 것으로 예측되었지만 실제로 2년간 범죄를 저지른 경우가 백인이 48%로 흑인 28%보다 훨씬 높았던 것으로 드러남. 프로퍼블리카 관련 보도 참조. Propublica, 2016.5.23., "Machine Bias-There's software used across the country to predict future criminals. And it's biased against blacks", <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

493) 가디언 관련 보도 참조. GUARDIAN, 2020.8.13., "Who won and who lost: when A-levels meet the algorithm", <https://www.theguardian.com/education/2020/aug/13/who-won-and-who-lost-when-a-levels-meet-the-algorithm>.

부정수급 소지가 있는 사람들을 발견하고자 하였으나[494], 이 시스템에 대하여 유엔 빈곤과 인권에 관한 특별보고관은 적법절차 보장 없이 저소득층, 이민자 및 소수민족에게 불리하게 사용되었다고 비판하였다[495].

이에 특히 공공부문 의사결정에 사용되는 인공지능에 대하여 차별금지법 등 인권관련 법과 규범에 근거한 개입과 권리구제 요구가 커지고 있다.

영국 공직생활윤리위원회는 2020년 보고서[496]에서 모든 공공기관 인공지능이 현행 법률을 준수하고 이를 공표하도록 권고하고, 영국 평등인권위원회에 공공부문 인공지능의 평등법 준수지침 개발을 요청하였다.

호주 국가인권위원회는 2019년 토론서[497]에서 호주 정부가 인공지능 정보 기반 의사결정 시스템의 도입을 계획할 경우 (a)인공지능 사용에 대한 비용 편익 분석을 수행하며 특히 인권 보호 및 책무 보장과 관련하여 살펴보고 (b)가장 영향을 받을 가능성이 높은 사람들에 초점을 맞춘 공청회를 개최하고 (c)법률에 명시되고 적절한 인권 보호가 이루어진 경우에만 시스템을 도입할 것을 제안하였다. 또 호주 정부 조달 규칙이 정부가 조달하는 인공지능 정보 기반 의사결정 시스템에 적절한 인권 보호를 포함하도록 요구할 것을 제안하였다. 인공지능 정보 기반 의사결정이 이루어진 경우 영향을 받은 사람에게 정보를 제공하고 그 설명가능성을 보장하는 법안 마련을 호주 정부에 제안하고, 인공지능 정보 기반 의사결정과 관련하여 호주에 적용되는 모든 표준이 인권 준수에 대한 지

494) 네덜란드 헤이그 지방법원은 2020년 2월 SyRI 관련 법률의 프라이버시 보호조치가 충분치 않고 그 작동 원리에 대한 "투명성이 중대하게 결여되어 있다"며 사용 중단을 명령하였다. 가디언 관련 보도 참조. GUARDIAN, 2020.2.5., "Welfare surveillance system violates human rights, Dutch court rules", <https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules>; 공익소송단 홈페이지 참조. PILP, 2020.2.5., "Landslide victory in SyRI-case: Dutch court bans risk profiling", <https://pilpnjcm.nl/en/landslide-victory-in-syri-case-dutch-court-bans-risk-profiling/>.

495) 유엔 빈곤과 인권에 관한 특별보고관 보도자료 참조. OHCHR, 2019.10.16., "The Netherlands is building a surveillance state for the poor, says UN rights expert", <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25152&LangID=E>.

496) The Committee on Standards in Public Life(2020), Artificial Intelligence and Public Standards.

497) Australian Human Rights Commission(2019), Human Rights and Technology : DISCUSSION PAPER.

침을 포함할 것 또한 요구하였다. 나아가 인권 중심 설계(human rights by design) 및 자율적·법적 인증제도의 검토를 요구하고 인권영향평가의 개발과 법규화 또한 제안하였다.

유럽평의회 인권위원장은 2019년 5월 인공지능에 대한 인권 규제 준수에 대한 보고서에서 각국 인공지능 시스템의 발전과 구현에 있어 특히 중대하게 영향을 받는 이해관계자들의 인권 보장을 요구하였다[498]. 이를 위해 인권위원장은 인권영향평가의 실시를 위한 법제도를 마련하고 이를 공공기관 조달에 반영할 것을 요구하였다. 더불어 인공지능의 인권 준수를 독립적이고 효과적으로 감독하기 위한 법제도를 마련하고, 개인정보 보호 및 프라이버시, 표현의 자유, 집회결사의 자유, 노동권 나아가 권리구제 보장을 요구하였다. 인권위원장은 인공지능 시스템이 그 차별을 방지하기 위하여 높은 수준의 정밀검사를 받아야 하며, 특히 인공지능으로부터 그 권리에 부당한 영향을 받을 위험성이 큰 사회집단(아동, 노인, 장애인 등)에 대한 차별을 방지해야 한다는 점을 강조하였다.

인공지능의 인권적 규제와 감독의 중요성이 커질수록 이 분야 국가인권기구의 역할과 개입에 대한 기대 또한 커지고 있다.

유럽연합 기본권청은 국가인권기구의 강화 및 효과적인 활동에 대한 최근 보고서[499]에서 인공지능 기술의 발전으로 사생활권, 개인정보 보호권, 차별금지 관련 조항이 동반하여 문제가 되고 있다고 지적하면서, 이 문제에서 독립성, 전문성 및 진정사건 처리 경험을 보유하고 있는 국가인권기구들이 알맞은 역할을 수행할 수 있다고 보았다. 예컨대 유럽연합 인공지능 윤리 가이드라인의 경우 "불공정한 편향이나 차별 등 인공지능 시스템에서 발생하는 유해한 결과"를 확인할 수 있도록 인공지능 시스템에 대한 '감사 메커니즘'을 권고하였으며, 국제인권법 의무 준수에 대한 감독 필요성을 제기하였다. 이러한 상황에서 독립적인 지위 및 인권에 관한 전문성을 보유한 국가인권기구 및 평등기구가 기여할 수 있는 역할이 있을 것이라고 기본권청은 강조한다.

인공지능 기술의 발전은 국가인권기구의 권리구제 활동에도 변화를 가져올 수 있기

498) Council of Europe Commissioner for Human Rights(2019), Unboxing artificial intelligence: 10 steps to protect human rights.

499) European Union Agency for Fundamental Rights(FRA)(2020d), Strong and Effective national Human Rights Institutions: Challenges, Promising Practices and Opportunities. 특히 3.4.1.절(인공지능: 과제 및 기회) 참조.

때문에 이 분야 국가인권기구의 대응은 필연적이다. 우선 알고리즘 의사결정으로 영향을 받은 개인들의 국가인권기구 진정 접수가 증가할 수 있으며, 국가인권기구는 알고리즘에 의한 개인정보 처리에 대해 이해하지 못하고 구제 곤란을 겪는 개인들을 위해 이해도 증진 활동에 개입해야 할 수 있다. 또한 국가인권기구 내부적으로도 알고리즘 의사결정에 대한 디지털 리터러시 향상 및 전문가 자문 네트워크 구축이 필요하고, 인공지능에 대한 총체적 접근을 위해서 다양한 행위자, 기관, 학계에 걸쳐 광범위하게 협업할 필요가 있다. 여기에는 개인정보 보호 감독기관을 비롯해 인공지능 관련 감독 기능을 가진 기존 기관과의 협력이 포함된다.

국제적으로 권위 있는 개인정보 보호 감독기관 국제협회는 2018년 발표한 <인공지능 윤리 및 개인정보 보호에 대한 선언>에서 개인정보 보호 감독기관들이 인권기구들과 협력할 필요성이 있다고 강조하였다[500]. 인공지능 분야에서 이루어지는 개인정보의 수집, 이용, 공개가 차별, 표현 및 정보의 자유 등 보다 광범위한 인권에 직접 영향을 미친다는 사실을 인식함에 따라, 개인정보 보호 및 프라이버시 감독기관들이 인권을 보다 광범위하여 고려하면서 다른 인권기구들과 협력해야 한다는 것이다.

최근 각국 국가인권기구들의 인공지능 정책 관련 개입도 증가하고 있다. 뉴질랜드 국가인권기구는 2018년 유엔 인권최고대표실에 <프라이버시, 데이터 및 기술: 디지털 시대 인권 문제> 보고서를 제출하고 디지털시대 인권 보호에 대한 일차적인 책임은 정부에 있다고 지적하고, 인공지능 기술 개발에 있어 유엔 기업과 인권 이행지침(UNGPs)에서 제시한 기업의 인권존중 책무 또한 커졌다고 강조하였다[501]. 네덜란드 국가인권기구는 <전략 계획 2020-2023>의 핵심 주제 중 하나로 “디지털화와 인권”을 채택하고 디지털 채용 절차에서 나타날 수 있는 노동 시장 차별 가능성에 대해서 검토하면서 동등한 대우를 받을 권리를 강조했다. 스웨덴 국가인권기구와 평등 옴부즈만은 인공지능의 차별금지법 준수를 감독하고 있다(FRA, 2020: 92).

특히 인공지능에 대해 요구되는 인권영향평가 및 인권 준수의 독립적인 감독에 있어

500) International Conference of Data Protection and Privacy Commissioners(2018), Declaration on Ethics and Data Protection in Artificial Intelligence 참조. 이 협회는 최근 세계프라이버시연맹(Global Privacy Assembly, GPA)으로 전환하였다.

501) New Zealand Human Rights Commission(2018), Privacy, Data and Technology: Human Rights Challenges in the Digital Age.

서 국가인권기구의 역할이 주목된다. 앞서 살펴본대로 유엔 의사표현의 자유 특별보고관, 유엔 인권최고대표실, 호주 국가인권위원회, 유럽평의회 인권위원장이 인공지능에 대한 인권영향평가의 실시를 각국 정부에 권고하였고, 호주 국가인권위원회와 유럽평의회 인권위원장은 인권영향평가를 법률적 수준으로 보장하고 공공조달 절차를 통하는 공공기관 인공지능의 경우 인권영향평가를 반드시 적용할 것을 정부에 요구하였다. 나아가 유럽평의회는 인공지능 인권영향평가에 대한 평의회 전체 권고를 추진 중이다[502]. 유엔인권최고대표실이 2020년 5월 28일 "인공지능, 프로파일링, 자동화된 의사결정, 머신러닝 기술이 적절한 보호조치가 없을 경우 프라이버시권의 향유에 미치는 영향"에 대하여 개최한 온라인 전문가 세미나에서도, 다수의 인권 전문가들이 인공지능에 대한 '핵심적인 보호조치'로서 인권영향평가 실시를 지지하였다. 특히 테러리즘에 대응 시 인권과 기본적 자유의 증진 및 보호에 관한 특별보고관(Ni Aolain)은 각국 정부에 대하여 인권영향평가의 엄중한 실시를 권고하였으며, 데이터 집중 시스템은 법적 목적 달성을 위한 필요성과 비례성이 입증되었을 때에만 도입될 수 있다고 강조하였다[503]

인공지능의 인권 준수에 대한 독립적인 감독의 필요성에 대한 요구 또한 커지고 있다[504]. 유엔 의사표현의 자유 특별보고관은 2018년 보고서에서 정부가 인공지능 시스템을 사용하는 경우 외부의 독립적인 전문가로부터 정기적인 감사를 받을 것을 권고하였고, 유럽평의회 인권위원장은 2019년 보고서에서 인공지능의 인권 준수에 대한 독립적이고 효과적인 감독을 위해 관련 법제도를 마련할 것을 회원국에 권고하였다. 독립적인 기구가 인권 준수 여부를 조사하고 영향을 받은 개인 진정을 처리하고 인공지능 시스템의

502) 자동화된 개인정보 처리 및 인공지능의 인권 문제 전문위원회가 2019년 11월 권고 초안을 발표하였다. Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence(MSI-AUT)(2019), Addressing the impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, <https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf>.

503) OHCHR(2020), Report of the proceedings of the online expert seminar, <https://www.ohchr.org/Documents/Issues/DigitalAge/ExpertSeminarReport-Right-Privacy.pdf>.

504) 특히 향후 인공지능을 활용한 행정이 확대될 경우 이러한 인공지능행정 알고리즘이 법령의 내용을 충실히 반영하고 있는지, 데이터 내용이나 알고리즘 프로그램이 합헌성을 유지하고 있는지에 대한 전문화된 검증 기관이 필요하다는 주장이 있다. 김두승(2019), 인공지능 기반 자동행정과 법치주의, 미국헌법연구 30권 1호, pp105-138.

성능 발전에 따른 정기적인 검토를 수행할 수 있도록 해야 한다는 것이다. 호주 국가인권위원회는 2019년 토론서에서 호주 정부의 인공지능에 대하여 새로운 기관 또는 기존 기관이 인권적 검토를 수행하여 이때 ▲ 정부가 의사결정 시 인공지능을 사용하는지 여부를 확인하고 ▲ 인공지능 사용에 대한 비용편익 분석은 물론 인권 보호 및 책무성 보장을 특별히 살펴보며 ▲ 인권영향평가를 비롯하여, 정부가 인공지능을 사용하는 의사결정 시스템을 채택하기로 결정하기까지 절차를 개괄하고 ▲ 의사결정으로 영향을 받는 사람에게 인공지능 사용에 대해 설명하는지 여부, 가장 영향을 받을 가능성이 높은 사람들에 초점을 맞춘 공청회를 실시하는지 여부 등 설명 방법에 대하여 확인하며 ▲ 의사결정 인공지능 사용에 대한 감시 및 평가 체계를 검토할 것을 호주 정부에 권고하였다. 호주 인권위원회는 정부 인공지능에 대한 검토와 별도로 전문적이고 독립적인 법정기구로 인공지능 안전위원회(AI Safety Commissioner)를 설립하여 국가 전반적으로 인공지능으로 인한 개인 및 지역사회의 피해를 방지하고 인권을 보호하고 증진하는데 주력하도록 제안하였다.

이상과 같이 공공부문을 비롯한 인공지능에 대하여 요구되고 있는 인권영향평가의 기준 마련 및 실시, 인공지능의 인권 준수에 대한 독립적인 감독 체계에 있어서 국가인권기구가 주무 또는 협의기구로서 기능할 수 있을 것이다. 우리의 국가인권위원회는 국제인권규범에 따라 설립된 국가인권기구로서 국가기관, 지자체의 인권침해에 대한 조사 및 구제, 인권정책 개선 권고 등을 소관해 왔고 차별 및 평등권 침해 행위에 대해서는 기업 등 사인에 대해서도 조사 및 구제 기능을 가지고 있다. 이러한 국가인권위원회의 기능에 기반하여 사회 각 부문에 도입되는 인공지능에 대하여 인권적 개입이 일정 정도 가능할 것이며, 특히 공공부문 인공지능에 대해서는 인권 기준 준수를 요구하는 활동이 신속히 이루어질 필요가 있다.

2. 국내 국가인권위원회와 개인정보 보호 활동

우리나라 국가인권위원회는 인권침해, 차별행위 및 성희롱에 대한 조사와 구제업무를 수행하고 있으며, 위원회가 진정을 조사한 결과 인권침해나 차별행위가 일어났다고 판단한 때에는 피진정인, 그 소속기관·단체 또는 감독기관의 장에게 인권침해나 차별행위의

중지, 원상회복·손해배상 등 그 밖에 필요한 구제조치, 재발 방지를 위해 필요한 조치, 법령·제도·정책·관행의 시정 또는 개선 등의 권고를 할 수 있다. 위원회의 조사업무 대상은 국가기관, 지방자치단체, 각급학교, 공직유관단체 또는 구금 ·보호시설의 업무수행과 관련하여 「헌법」 제10조부터 제22조까지의 규정에서 보장된 인권을 침해하거나 차별한 행위, 법인, 단체 또는 사인(私人)으로부터의 차별행위이다. 특히 위원회는 헌법 제10조 및 제17조에서 보호하고 있는 사생활권 및 개인정보 보호 권리의 침해에 대하여 구제해 왔다. 위원회가 소관하는 차별행위는 합리적인 이유 없이 성별, 종교, 장애, 나이, 사회적 신분, 출신지역, 출신국가, 출신민족, 용모 등 신체조건, 혼인여부, 임신 또는 출산, 가족형태 또는 가족상황, 인종, 피부색, 사상 또는 정치적 의견, 형의 효력이 실효된 전과, 성적(性的) 지향, 병력(病歷) 등을 이유로 고용, 재화·용역·교통수단·상업시설·토지·주거시설의 공급이나 이용, 교육시설이나 직업훈련기관에서의 교육·훈련이나 그 이용과 관련하여 특정한 사람을 우대·배제·구별하거나 불리하게 대우하는 행위이다. 그 외에도 위원회는 「장애인 차별금지 및 권리구제 등에 관한 법률」, 「고용상 연령차별금지 및 고령자 고용촉진에 관한 법률」에 따라 장애인 차별과 연령 차별도 조사한다.

국가인권위원회 통계에 따르면[505] 2001년부터 2018년까지 접수된 기관별 인권침해 상담건수 총 143,304건 중 다수인보호시설이 가장 많은 65,517건(45.72%), 경찰이 28,485건(19.88%) 순으로 나타났다. 전체 구금·보호시설을 모두 합할 경우 69,651건으로 무려 전체의 48.60%를 차지하고, 검찰, 경찰, 국정원, 특사경 등 수사기관을 모두 합할 경우 33,582건으로 전체의 23.43%를 차지한다. 2001년부터 2018년까지 접수된 기관별 인권침해 진정건수의 경우도 유사하다. 총 101,147건 중 다수인보호시설이 가장 많은 29,686건(29.3%), 경찰이 24,841건(24.6%) 순으로 나타났다. 전체 구금・보호시설을 모두 합할 경우 31,426건으로 무려 전체의 31.07%를 차지하고, 검찰, 경찰, 국정원, 특사경 등 수사기관을 모두 합할 경우 29,318건으로 전체의 28.99%를 차지한다.

한편, 2001년부터 2018년까지 주요기관의 인권침해 유형별 상담 현황을 살펴보면, 전체 62,876건 중 도·감청(173건), 피의사실 유포/개인정보 관리(2,828건) 등 사생활 및 개인정보 관련 인권침해 상담 및 진정이 3,001건으로 전체의 4.77% 건을 차지하고 있다.

505) 국가인권위원회(2018), 2018 국가인권위원회 통계.

<표7-1> 국가인권위원회 접수 인권침해 현황

구분	상담건수	진정건수
합계	143,304	101,147
검찰	4,746	3,008
경찰	28,485	19,833
국정원	243	258
특사경	108	169
지방자치단체	8,964	4,734
사법기관	2,015	1,207
입법기관	94	76
기타국가기관	9,276	7,503
구금시설	3,965	29,686
다수인보호시설	65,517	24,841
군	4,524	2,280
각급학교	7,459	4,143
출입국관리기관	471	397
보호시설	169	0
공직유관단체	2,904	1,441
기타	4,364	1,571

* 출처: 국가인권위원회(2018), 2018 국가인권위원회 통계 재구성(이하 같음).

<표7-2> 주요기관 사생활/개인정보 관련 인권침해 접수 현황

기관	구분	도 · 감청 등	피의사실 유포/개인정보 관리 등	소계	전체
검찰	상담	13	263	276	4,746
	진정	6	106	112	3,008
경찰	상담	105	1,484	1,589	28,485
	진정	37	744	781	19,833
군	상담	6	153	159	4,524
	진정	6	78	84	2,280
합계		173	2,828	3,001	62,876

<표7-3> 국가인권위원회 접수 차별행위 현황

구분	상담	진정	구분	상담	진정
합계	32,026	28,748	임신/출산	536	304
성별	992	972	가족상황	243	223
종교	253	209	인종	56	118
장애	10,715	13,524	피부색	18	17
나이	1,996	1,719	사상/정치적의견	101	57
사회적신분	2,620	2,317	전과	415	227
출신지역	205	171	성적지향	74	352
출신국가	740	429	병력	925	455
출신민족	39	18	학별/학력	375	649
용모/신체조건	466	356	성희롱	8,292	2737
혼인여부	182	141	기타	2,783	3,753

또한 2001년부터 2018년까지 차별행위에 대한 상담 및 진정건수는 각각 32,026건과 28,748건에 달한다.

제3절 시사점

개인정보 보호법의 제정과 개정을 거치면서 국내 개인정보 보호 감독체계는 그 독립성과 효과성을 강화하는 방향으로 개선되어 왔다. 그러나 현행 개인정보 보호 감독체계는 정보주체의 보호 면에서 몇 가지 중대한 한계를 가지고 있다.

우선 금융기관 개인정보 처리가 개인정보 보호위원회의 감독에서 분리되어 있고, 국가안전보장 관련 개인정보 처리에 대해서도 포괄적으로 그 적용을 제외하고 있다. 반면 유럽 및 유엔 등 국제 규범에서는 금융기관의 개인정보 처리를 분리하는 경우를 발견할 수 없고, 국가안전보장과 관련한 개인정보 처리의 경우 그 특수한 예외를 인정하면서도 원칙적으로 법률에 따라 제한하도록 하고 독립적이고 효과적인 감독을 권장하고 있다.

국제규범에 부합하는 효과적이고 독립적인 개인정보 보호 감독체계를 수립하기 위하여 신용정보법의 개인정보 관련 조항을 개인정보 보호법으로 일원화하고 금융위원회의 개인정보 감독권한을 개인정보 보호위원회로 이관하는 것이 바람직하다. 또한 국가안전보장 목적으로 개인정보 보호규범의 적용을 일부 제외하더라도, 개인정보 보호법 혹은 별도의 법률을 통해, 대상 개인정보의 수집·이용의 목적, 개인정보의 항목, 조치 업무 및 그 대상자의 범위, 안전성 확보 조치, 개인정보 처리자의 명시, 개인정보의 보유 및 이용기간, 정보주체에 대한 고지와 권리 행사 및 예외 등에 관해 구체적으로 규정해야 한다.

현행 개인정보 보호와 감독체계에 있어서 가장 큰 미비점은 범죄수사 및 형집행 등과 관련한 개인정보 처리에 대하여 매우 광범위한 예외를 두고 있다는 점이다. 범죄수사나 형집행 관련 기관들은 공공기관이 보유하고 있는 개인정보에 대하여 특별한 요건이나 절차 없이 제공받을 수 있는데 이러한 제공 및 처리 대상에 민감정보와 고유식별정보도 광범위하게 포함되어 있다. 범죄수사 및 형집행 등과 관련된 개인정보파일의 경우 감독기관에 대한 등록 및 공개가 면제되어 있고 개인정보 처리방침도 수립 및 공개 의무가 없어 개인정보 보호 감독에서 전면적으로 제외되어 있다. 정보주체의 열람 및 정정·삭제권과 처리정지권의 행사, 정보주체의 고지 받을 권리 역시 동반하여 제한되어 있어 정보주체의 권리 침해에 대한 인지와 권리구제가 상당히 어려운 상황이다.

문제는 이상과 같은 국내 개인정보 보호 감독체계의 한계가 현행 개인정보 보호법의 규정과 운용상 한계에서 유래했다는 점이다. 따라서 현행 개인정보 보호법에 따라 이루어지는 이 분야 개인정보 보호위원회의 감독과 권리구제에도 한계가 있을 수밖에 없다. 궁극적으로는 유럽연합 경찰 디렉티브 등 국제규범에 부응하는 입법적인 개선이 이루어져야 하겠지만, 장기간 이 분야 정보주체의 권리구제를 방대한 예외 상황 속에 방치할 수 없는 상황이다. 현행 제도 속에서 국가인권기구의 기능을 통해 가능한 감독 방안을 모색해 볼 필요가 있다.

우리나라 국가인권위원회는 국제 규범에 부합하는 독립적인 국가인권기구로서 국제규범과 헌법, 인권 관련 법률에 기반한 침해 조사와 구제 등 인권 관련 업무를 전문적이고 광범위하게 수행해 온 국가기관이다. 위원회는 헌법 제10조 및 제17조 침해 행위에 대한 조사와 구제 업무를 통하여 개인정보 보호 분야 경험과 전문성을 축적해 왔다. 국가인권기구와 개인정보 보호 감독기관 간에 긍정적인 상호작용을 모색해 온 유럽의 사례

를 참고해 본다면, 현행 개인정보 보호법의 한계로 인한 감독 및 권리구제의 미비점을 국가인권위원회 업무를 통해 보완해 볼 수 있을 것이다[506].

특히 국가인권위원회가 침해 조사 및 구제의 주요 대상인 구금·보호시설 및 수사기관의 개인정보 침해 사건에 대한 조사 및 구제 활동을 보다 강화한다면, 현행 개인정보 보호법에서 광범위하게 제외되고 있는 범죄수사 및 형집행 관련 개인정보 처리에 대한 권리구제가 보완될 수 있다. 위원회는 개인정보 보호법의 제한으로 공개되어 있지 않은 경찰의 채증자료의 인권 침해 사건에 대하여 이미 여러 차례 진정을 수리하고 조사 후 주의조치 등 권리구제에 임한 바 있다[507]. 나아가 채증 관련 제도의 개선을 위하여 그 수집·사용·보관·폐기와 관련한 절차의 객관성과 투명성을 제고하고 외부전문가가 참여하는 채증자료 관리 절차를 마련할 것을 정책적으로 권고한 바도 있다[508].

한편, 오랜 기간 차별 시정의 경험을 축적해온 국가인권위원회는 인공지능으로 인한 차별 시정 및 권리구제에 있어서 다른 기관보다 강점을 가지고 있다. 알고리즘 기반 의사결정의 정보인권 침해 문제는 개인정보 보호권 침해에 그치지 않으며 그 인권침해 및 차별에 대하여 국가인권기구의 종합적인 접근과 시정이 필요하다. 만약 알고리즘이 고용, 상업 및 공공서비스의 제공에 있어서 합리적인 이유 없이 성별, 장애, 나이, 출신지역, 출신국가, 출신민족, 용모 등 신체조건, 인종, 전과, 병력 등을 이유로 배제, 구별, 불리하게 대우할 경우 위원회가 조사와 구제업무를 수행할 수 있을 것이다.

최근 국제적으로 인권침해 우려가 증가하고 있는 인공지능 기술에 대하여 각국 국가인권기구들의 보다 적극적인 역할이 요구되고 있다. 우리 국가인권위원회는 인권에 관한

---

506) 다만 유럽연합은 개인정보 보호 감독기관과 타 국가기관 간에 상호협력을 규정하고 있다는 점에서 우리의 상황과 차이가 있다. 유럽연합 GDPR에서는 개인정보 보호 감독기관에 대한 진정인으로 정보주체를 대리하는 비영리단체, 기관 또는 협회를 광범위하게 인정하고 있으며 국가인권기구를 비롯한 다른 국가기관도 진정 주체에 포함될 수 있다는 것이 유럽연합 EDPS의 해석이다(Hustinx, 2013). 반면 우리나라에서 「민원 처리에 관한 법률」에 따른 "민원인"이란 “행정기관에 민원을 제기하는 개인ㆍ법인 또는 단체”이며, 국가인권위원회법에 따라 위원회에 진정할 수 있는 주체는 “대한민국 국민과 대한민국 영역 안에 있는 외국인으로서 인권침해나 차별행위를 당한사람(피해자) 또는 그 사실을 알고 있는 사람이나 단체”이다. 우리나라 현행 제도 하에서는 국가기관이 정보주체를 대리하여 권리구제 민원이나 진정을 제기하는 주체에 해당할 수 있을지는 모호한 상태이다.

507) 국가인권위원회 2005.2.14. 결정 03진인5400, 03진인6412, 04진인6, 04진인2696 (병합); 국가인권위원회 2009.12.7. 결정 09진인3456; 국가인권위원회 2013.9.30. 결정 13진정026160 참조.

508) 국가인권위원회 2014.4.3. 결정, 집회 및 시위현장에서 경찰의 채증관련 제도개선 권고 참조.

전반적인 문제를 다루는 기구로써 인권에 관한 법령, 제도, 정책, 관행의 조사와 연구 및 개선이 필요한 사항에 관한 권고 또는 의견 표명을 임무로 해 왔다. 이 분야에서는 유럽연합 기본권청이 인공지능 등 신기술이 기본권에 미치는 문제를 특수주제 업무로 정하고 신속한 의견을 통해 모범 규범을 주도해 왔다는 사실을 참고해 볼 만 하다. 위원회 역시 향후 인공지능을 비롯한 신기술에 관한 법령, 제도, 정책, 관행의 인권적 영향에 대하여 보다 적극적인 조사, 연구, 권고 또는 의견 표명에 나설 필요가 있다. 위원회는 2020년 「인공지능산업 진흥에 관한 법률안」에 대한 의견을 표명하고 인공지능에서의 인권 및 인간존엄성 존중 원칙, 인공지능으로 인한 차별 방지 원칙에 관한 규정과 기본계획 수립 시 포함되어야 할 사항으로 인권보호에 관한 사항이 추가로 규정될 필요가 있다는 의견 표명을 통해 인공지능 문제에 대한 검토를 이미 수행한 바 있다[509]. 위원회가 수행해 온 인권 교육 및 홍보 활동을 통해서도 인공지능 등 신기술의 인권 문제에 대한 사회적 인식 제고에 기여할 수 있는 바가 있을 것이다. 최근 국제적으로 제안되고 있는 인공지능 인권영향평가의 기준 마련 및 실시, 인공지능의 인권 준수에 대한 독립적인 감독 기구로서 역할 또한 검토해 봄직하다.

509) 국가인권위원회 2020.4.2. 결정, 「인공지능산업 진흥에 관한 법률안」에 대한 의견 참조.

제8장 결론 및 정책권고

전 세계 각국은 빅데이터, 인공지능 등 신기술 발전에 대응하기 위해 자국의 개인정보 보호 법제를 개선하고 있다. 우리나라에서도 몇 년 전부터 빅데이터 시대 개인정보 규범의 재정립을 둘러싼 논란이 첨예했으며, 그 결과 2020년 1월 소위 '데이터 3법'이 국회를 통과했지만 여전히 법제 정비가 미흡한 상황이다.

개인정보 보호법 개정 과정에서 많은 사람들이 '보호와 활용의 조화'를 주장했지만, 개인정보의 활용을 위한 보호의 타협으로 귀결되었다. 정보주체의 권리를 보호하지도 못하면서 개인정보처리자와 정보주체 모두에게 불필요한 부담만 야기하는 규제가 있다면 당연히 재검토되어야 한다. 그러나 개인정보의 활용을 명분으로 정보주체 권리 보호를 약화시켜서는 안 된다. 보호와 활용의 조화는 보호와 활용이라는 양극단의 중간 타협점을 찾는 과정이 아니다. 보호와 활용이 동전의 양면인 이유는 개인정보 보호의 기준이 결국 활용의 기준이 되기 때문이다. 예를 들어 동의는 정보주체의 선택권을 보장하는 방편이면서 (활용을 막고자 하는 것이 아니라) 활용을 위한 조건인 것이다. 신기술의 발전을 저해하는 것은 오히려 그 기준 자체가 모호한 점에 있다. 따라서 급속히 변화하는 신기술 환경에서 위험 요인을 이해하고 정보주체의 권리를 보호하기 위한 새로운 기준을 설정할 필요가 있다. 이는 동시에 개인정보의 안전한 활용을 위한 기준이 될 것이다.

내 개인정보가 안전하게 관리될 것이라는 정보주체의 신뢰가 없다면 새로운 산업의 발전도, 새로운 공적 서비스의 도입도 불가능하다. 소비자의 신뢰가 없다면 새로운 서비스는 개인정보의 상품화에 불과할 것이다. 시민의 신뢰가 없다면 정부가 도입하는 신기술은 새로운 국가 감시 시스템에 불과할 것이다. 기술의 발전과 도입 과정에서 개인정보 자기결정권을 비롯한 기본권을 중심에 두어야 할 필요가 여기에 있다.

이에 결론을 대신하여 신기술 환경에서 정보주체의 권리를 보호하고 개인정보의 안전한 활용을 위한 개선 방향을 다음과 같이 권고하고자 한다.

1. 정보주체의 권리 보호를 위한 정책 권고

다음과 같은 정보주체의 권리가 보장될 수 있도록 개인정보 보호법을 개선해야 한다.

가. 정보주체는 자신의 개인정보가 어떻게 처리되는지에 대해 고지 받을 권리를 가진다. 동의를 받을 때뿐만 아니라, 계약이나 정당한 이익 등 다른 적법 근거에 따라 개인정보가 수집될 경우에도, 정보주체로부터 개인정보를 직접 수집한 때뿐만 아니라 간접적으로 개인정보를 획득할 경우에도 개인정보처리자는 정보주체에게 개인정보 처리와 관련한 정보를 제공해야 한다. 정보주체에게 제공되는 정보는 처리의 주체, 목적, 방법뿐만 아니라 정보주체가 어떠한 권리를 행사할 수 있는지, 자신의 권리가 침해되었을 때 어떻게 구제받을 수 있는지도 포함해야 한다.

나. 정보주체에게 개인정보의 처리와 관련한 내용을 고지할 때에는 정확하고, 투명하며, 이해하기 쉬운 형식으로 명확하고 평이한 언어를 사용하여야 한다.

다. 정보주체는 개인정보처리자가 보유하고 있는 자신의 개인정보에 대한 열람·정정·삭제권을 가진다. 그러나 정보주체의 정정·삭제권이 열람권 행사를 전제로 하는 것은 아니다.

라. 정보주체는 자신의 개인정보의 처리 방법, 처리 여부에 대해 알 권리를 가진다. 또한 자신이 동의한 개인정보의 처리에 대해서는 동의를 철회할 권리, 동의가 아닌 다른 법적 근거에 의한 개인정보의 처리에 대해서는 자신이 원하지 않을 경우 처리의 정지를 요구하거나 반대할 권리를 가진다.

마. 과학적 연구·통계 작성·공익적 기록보존 목적으로 개인정보를 가명처리하거나 가명처리된 개인정보를 활용하는 경우에도 정보주체의 권리는 존중되어야 한다. 다만, 정보주체의 권리를 보장하면 처리 목적의 달성이 불가능하거나 중대하게 손상되는 경우, 혹은 권리의 보장이 불가능하거나 매우 과도한 노력을 요하는 경우에 한하여 정보주체의 권리를 제한할 수 있다.

바. 정보주체는 개인정보처리자에게 제공한 자신의 개인정보를 체계적이고 기계 판독이 가능한 형식으로 제공받을 권리 및 다른 개인정보처리자에게 해당 개인정보를 이전할 권리(개인정보 이동권)를 가진다.

사. 정보주체는 프로파일링 등, 본인에 관한 법적 효력을 초래하거나 이와 유사하게 본인에게 중대한 영향을 미치는 자동화된 처리에만 의존하는 결정의 적용을 받지 않을 권리를 가진다. 또한 자동화된 의사결정의 유무, 관련한 로직과 정보주체에 미치는 중대한 영향에 대한 정보를 제공받을 권리를 가진다. 예외적으로 자동화된 의사결정이 이루어지는 경우 정보주체는 인적 개입 요구권, 의견 진술권, 이의제기권을 보장받아야 한다.

아. 이해하기 쉽고 평이한 문구를 사용하거나 아이콘 등을 활용하여 정보주체가 단순하고 명확하게 중요 내용을 이해할 수 있도록 하는 등, 정보주체의 동의가 실질적으로 정보에 기반한(informed) 동의가 될 수 있도록 해야 한다. 소비자단체, 개인정보 보호위원회, 소비자보호원 등 전문기관들이 정보주체를 대신하여 주요 개인정보처리자의 약관이나 개인정보 처리방침에 문제가 없는지 검토하고 인증하도록 하는 것도 하나의 대안이 될 수 있다.

2. 개인정보 처리자의 책임성 강화를 위한 정책 권고

정보주체의 권리가 실제로 보호되기 위해서는 개인정보 처리 주체인 개인정보 처리자의 책임성이 무엇보다 중요하다. 개인정보 처리자의 책임성을 강화하는 방향으로 개인정보 보호법을 개선해야 한다.

가. 개인정보처리자가 개인정보 보호법을 준수하고 이를 입증할 수 있도록 하는 책임성 규정이 개인정보 보호원칙에 반영되어야 한다.

나. 개인정보처리자는 개인정보 보호법을 준수하고 이를 입증할 수 있는 기술적, 조직적 조치를 취해야 한다. 이러한 조치의 수준은 개인정보 처리의 위험성에 비례(위험 기반 접근)해야 한다.

다. 이러한 기술적, 관리적 조치는 개인정보의 처리 방법을 결정한 시점 및 그 처리가 이루어지는 해당 시점에 이행되어야 하며, 개인정보 보호원칙을 효율적으로 이행하고 필요한 안전조치가 개인정보 처리에 통합될 수 있도록 설계되어야 한다(개인정보 보호 중

심설계). 또한, 개인정보처리자는 특정 처리 목적에 필요한 최소한의 개인정보만 처리되도록 기본설정을 통해 적절한 기술적, 관리적 조치를 이행해야 한다(개인정보 보호 기본설정).

라. 개인정보처리자는 처리자의 신원, 처리의 목적, 처리되는 개인정보 등 처리 활동을 기록하고 보존해야 한다.

마. 개인정보 영향평가는 공공기관 뿐만 아니라 개인정보 처리의 위험성이 큰 민간분야로 확대되어야 한다. 영향평가의 수행 여부는 형식적인 기준이 아니라 실질적인 위험성을 기준으로 판단해야 하고, 개인정보 영향평가가 포함해야 할 최소한의 내용을 개인정보 보호법에 규정하며, 영향평가 과정에서 정보주체의 의견을 구하도록 한다. 영향평가에도 불구하고 위험을 억제하는 적절한 수단을 갖추지 못한 경우 개인정보 보호위원회에 자문을 구하도록 하는 절차를 둔다.

바. 현행 개인정보 보호법에서 규정하고 있는 개인정보 보호책임자와 별개로, 개인정보 처리자로부터 독립적인 지위를 갖고 개인정보처리자를 자문하고 감독할 독립 정보보호 책임자(DPO) 제도를 도입할 필요가 있다. 공공기관 및 개인정보 처리 위험성이 높은 민간 기업을 대상으로 전문성이 있는 자를 DPO로 선임하도록 한다.

사. 자발적인 참여에 기반한 인증 제도를 도입하되, 인증기준과 인증기관에 대한 승인 및 관리는 개인정보 보호위원회가 담당한다. 또한 각 분야별 개인정보처리자들이 고유한 규범을 ‘행위 규범’으로 구체화하고 독립적인 모니터링 기관을 통해 준수 여부를 확인하는 행위 규범 제도를 마련할 필요가 있다. 이 역시 개인정보 보호법 준수를 입증하는 하나의 방식이 될 수 있다.

3. 신기술 환경에서 인권 보호를 위한 정책 권고

빅데이터, 인공지능 등 신기술의 발전은 인간의 삶에 편의를 가져다주기도 하지만, 인권에 새로운 위험을 야기하기도 한다. 이에 따라 개인정보 보호 규범도 변화할 필요가

있는데, 앞서 언급한 정보주체의 권리 및 개인정보처리자 책임성 강화 방안은 이러한 신기술의 발전을 이미 고려한 것이다. 여기서는 그 외의 추가적인 정책 권고를 다룬다.

가. 과학적 연구와 통계 작성은 한 사회의 지식 기반을 확대하고 공공정책 및 산업발전에 유용하게 활용될 수 있다. 과학적 연구와 통계 작성을 목적으로 개인정보를 애초 수집한 목적 외로 활용할 필요성이 있으나, 개인정보의 목적 외 활용은 정보주체의 권리에 부정적인 영향을 미칠 수 있다. 따라서 과학적 연구와 통계 작성 목적은 정보주체의 권리 제한에 상응하는 공공적 가치를 가져야 한다. 해당 분야의 윤리 규범을 준수해야 하며, 그 결과물은 사회에 공유되어 모두가 향유할 수 있어야 한다.

나. 과학적 연구와 통계 작성 목적으로 안전하게 개인정보를 처리, 연계하기 위한 데이터 거버넌스 체제를 구축할 필요가 있다. 이는 과학적 연구의 공공적 가치를 판단하기 위한 심사위원회의 구성, 해당 목적을 위해 처리되는 개인정보 최소화를 위한 조치, 가명처리나 암호화를 포함하는 안전조치, 전송 및 보관 과정에서의 보안조치, 연구자에 대한 교육 및 훈련, 연구결과물이 개인정보를 침해할 우려가 없는지에 대한 검토, 개인정보 처리에 대한 공개 및 정보주체의 거부권 보장 방안 등을 포함한다.

다. 개인정보를 과학적 연구 및 통계 작성 등의 목적으로 애초 수집 목적 외로 추가 처리하더라도 데이터 최소화, 보관 제한 등 개인정보 보호원칙은 준수되어야 한다. 즉, 특정한 과학적 연구 및 통계 작성에 필요한 최소한의 개인정보만이 처리되어야 하고, 가능한 한 익명처리해야 하며, 특정 목적(특정한 과학적 연구 및 통계 작성 목적)이 다하면 해당 개인정보를 파기해야 한다.

라. 민감정보를 과학적 연구 및 통계 목적으로 활용할 경우, 법령에 근거해야 하고 해당 법률에서는 민감정보 처리에 필요한 안전조치를 규정해야 한다.

마. 인공지능 등 신기술은 개인정보 자기결정권 뿐만 아니라, 표현의 자유, 적법절차, 노동권, 평등권 및 차별받지 않을 권리 등 다른 기본권에 부정적 영향을 미칠 수 있다. 국가인권위원회는 신기술에 관한 법령, 제도, 정책, 관행의 인권적 영향에 대하여 적극적

인 조사, 연구, 권고 또는 의견 표명에 나서야 한다.

바. 최근 인공지능이 그 개발이나 사용 과정에서 편향된 학습으로 인해 성별, 인종, 빈곤 지역에 따라 사람을 차별한 사례가 드러났으며 인공지능의 사용이 확산됨에 따라 차별이 확산·증폭될 위험성이 있다. 인공지능은 개발되거나 사용되는 과정에서 그 알고리즘 및 데이터셋이 헌법과 차별금지 관련 법률들 및 국가인권위원회법이 보호하는 평등권과 차별금지 원칙을 침해하지 않아야 한다. 국가인권위원회는 인공지능의 차별에 대한 조사 및 권리구제에 나서야 하며, 차별을 방지하기 위한 인공지능 알고리즘, 데이터셋 및 그 결과에 대한 검증 기준 및 감독 체계를 개발하고 교육 및 홍보하여야 한다.

사. 인공지능이 기본권에 미치는 부정적 영향을 최소화하기 위해 인권영향평가를 시행할 필요가 있다. 특히 법적 또는 이와 유사하게 중대한 영향을 미치는 자동화된 의사결정에 사용되거나 공공기관이 도입하는 인공지능의 경우 인권영향평가가 의무화되어야 한다. 국가인권위원회는 인공지능에 대한 인권영향평가의 대상, 시기, 기준, 이행 방안 등에 대한 정책을 개발하고 이를 교육 및 홍보하는 한편, 인권영향평가의 제도화를 위하여 노력하여야 한다.

아. 독립적 인권기구로서 사생활의 비밀과 자유, 개인정보 자기결정권 등 기본권을 옹호할 의무가 있는 국가인권위원회와 개인정보 보호법에 근거를 두고 설립된 개인정보 감독기관인 개인정보 보호위원회는 신기술 발전에 따라 국민의 기본권이 침해되지 않고 보호될 수 있도록 협력해야 한다.

4. 개인정보 보호체계 효율화를 위한 정책 권고

수범자의 혼란과 비용을 최소화하기 위해서는 개인정보 보호체계를 효율화할 필요가 있다. 또한 개인정보의 국가 간 이전이 보편화되고 있는 상황에서 세계적으로 개인정보의 보호와 활용이 실효성을 갖기 위해서는 우리 개인정보 보호법을 국제규범에 맞게 개선할 필요가 있다.

가. 신용정보법, 위치정보법의 개인정보 관련 조항을 개인정보 보호법으로 일원화하고 금융위원회의 개인정보 감독권한을 개인정보 보호위원회로 이관해야 한다.

나. 국제 규범과의 조화를 위해, 현재 유일하게 구속력 있는 개인정보 관련 국제규범인 유럽평의회 108호 협약에 가입할 필요가 있다.

다. 유럽연합과는 일본의 사례와 같이 상호 적정성 결정을 체결할 필요가 있다. 이를 위해서 일본과 같이 보완 규정에 의존하는 것보다는 우리 개인정보 보호법을 GDPR과 동등한 수준으로 개선할 필요가 있다. 또한 우리 국민의 개인정보가 다른 나라에서도 보호받을 수 있도록 다른 나라 개인정보 보호 법제에 대한 적정성 판단을 포함한 개인정보 국외 이전 제도를 개선할 필요가 있다.

5. 정보기관 및 수사기관의 개인정보 처리와 관련한 정책 권고

지금까지 정보기관 및 수사기관의 개인정보 처리는 개인정보 보호법에서 예외를 인정받아왔다. 그러나 국가안보 및 범죄수사 등의 목적을 위해 일반적인 개인정보 처리규범으로부터 일정한 예외를 인정하더라도, 개인정보 보호의 사각지대가 되어서는 곤란하다. 정보기관 및 수사기관의 예외적인 개인정보 처리규범 및 개인정보 처리시스템의 구축 및 운영도 법률로서 명확하게 규정하여 규율할 필요가 있으며, 독립적인 감독기관의 감독을 받아야 한다.

가. 현행 개인정보 보호법은 범죄의 수사와 공소의 제기 및 유지를 위하여 필요하거나 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우, 개인정보의 목적 외 이용·제공 제한, 민감정보 및 고유식별정보의 처리 제한, 개인정보파일의 등록 및 공개, 개인정보처리방침의 수립 및 공개에 대하여 일률적으로 그 적용의 예외를 두고 있다. 특히 이와 동반하여 정보주체의 열람 및 정정·삭제권과 처리정지권의 행사, 정보주체의 고지 받을 권리 또한 일률적으로 배제하고 있다. 수사기관 및 구금시설의 개인정보 처리에 대한 개인정보 보호법의 일률적인 예외 규정들은 법률적인 개선이 필요하며 개인정보 보호위원회가 독립적인 감독을 수행하도록 해야 한다.

나. 국가안전보장 목적으로 개인정보 보호 규범의 적용을 일부 제외하더라도, 개인정보 보호법 혹은 별도의 법률을 통해, 대상 개인정보의 수집·이용의 목적, 개인정보의 항목, 조치 업무 및 그 대상자의 범위, 안전성 확보 조치, 개인정보 처리자의 명시, 개인정보의 보유 및 이용 기간, 정보주체에 대한 고지와 권리 행사 및 예외 등에 관해 구체적으로 규정해야 한다.

다. 국가인권기구인 국가인권위원회는 수사기관 및 구금시설의 개인정보 처리 및 정보주체의 권리 행사에 있어 부당한 침해가 발생하지 않도록 고유의 조사 및 권고의 기능을 발휘하여 일정한 수준의 감독권을 행사할 필요가 있다.

참 고 문 헌

1. 국내자료

[1] 개인정보보호위원회(2020), 가명정보 처리 가이드라인.

[2] 개인정보보호위원회(2020), 2020 개인정보보호 연차보고서

[3] 개인정보보호위원회, 보건복지부(2020), 보건의료 데이터 활용 가이드라인.

[4] 경찰개혁위원회(2018), 경찰의 정보활동 개혁 권고(연번 25).

[5] 고수윤(2020), GDPR과 CCPA상 정보주체 권리에 관한 비교법적 연구, 미디어와 인격 권 제6권 제1호.

[6] 고환경 외(2019), MyData 서비스의 개인동의 방식 개선 연구, 한국데이터산업진흥원 위탁연구보고서.

[7] 과학기술정책연구원(2006), 참여정부의 새로운 시도 : 정책 아키텍쳐 혁신.

[8] 국가인권위원회(2018), 2018 국가인권위원회 통계.

[9] 국가인권위원회(2020), 개인정보 보호법 시행령 일부개정령안 검토서.

[10] 권건보 외(2017), 지능정보사회 대응을 위한 개인정보보호 법제 정비방안, 개인정보보호위원회 연구용역보고서.

[11] 권영준(2015), 개인정보 자기결정권과 동의 제도에 대한 고찰, 2015 NAVER Privacy White Paper.

[12] 김경환(2016), [ICT법 바로알기 73] 일본 개인정보보호법과 빅데이터 목적의 익명가공정보(1)

[13] 김두승(2019), 인공지능 기반 자동행정과 법치주의, 미국헌법연구 30권 1호.

[14] 김재완(2019), EU 일반정보보호규정(GDPR)의 알고리즘 자동화 의사결정에 대한 통제로써 설명을 요구할 권리에 대한 쟁점 분석과 전망, 민주법학 제69호, 민주주의법학연구회.

[15] 김재환(2020), 데이터3법 시행령 개정안 정부 토론회 토론문.

[16] 김서안, 이인호(2019), 유럽연합과 미국에서의 개인정보이동권 논의와 한국에의 시사점, 중앙법학 제21집 제4호, 중앙법학회.

[17] 김일환(2017), 현행 개인정보보호법체계상 감독기구 법제정비방안에 관한 연구, 미국헌법연구 제28권 2호.
[18] 김현경(2020), 개인신용정보의 범위에 대한 비판적 고찰- 상행위 거래정보는 모두 개인신용정보인가?, 개인정보보호법학회 특별세미나(2020.10.12.) 발표문.
[19] 나종연(2013), 정보주체 동의권의 실질적 보장을 위한 연구, 서울대학교 산학협력단, 개인정보위원회 연구용역보고서.
[20] 박노형, 정명현(2018), EU GDPR상 프로파일링 규정의 법적 분석, 안암법학 56권, 안암법학회.
[21] 박상돈(2017), 헌법상 자동의사결정 알고리즘 설명요구권에 관한 개괄적 고찰, 헌법학연구 제23권 제3호, 한국헌법학회.
[22] 박훤일(2015), 유럽회의 108호협약의 의의와 우리나라 가입의 필요성, 경희법학 제50권 제4호.
[23] 손형섭(2012), 개인정보보호법의 특징과 앞으로의 방향- 업계의 반응에 대한 몇 가지 대안을 중심으로, 언론과 법.
[24] 손형섭 외(2017), 일본의 개인정보보호 법제·정책 분석에 관한 연구, 개인정보보호위원회 연구용역보고서.
[25] 손형섭(2019), 한국 개인정보보호법과 일본 개인정보보호법의 비교 분석- ICT산업 생태계에 미치는 영향을 중심으로, 2019 NAVER Privacy White Paper.
[26] 양기진(2019), 개인정보의 통계작성 · 연구 목적 활용에 관한 검토- GDPR의 관점상 김병욱 의원 대표발의 개정안의 비판적 검토를 중심으로 -, 법조 제68권 제5호(통권 제737호).
[27] 이광석 외(2018), 4차 산업혁명 시대에서 정보인권 보호를 위한 실태조사, 국가인권위원회 연구용역 보고서.
[28] 이규엽 외(2020), 미국 개인정보보호법 입법 동향: 국내 개정법과의 비교 및 시사점.
[29] 이대희(2015), 개인정보 개념의 해석 및 범위에 관한 연구, 고려법학 제79호.
[30] 이상경, 남정아(2017), 미국의 개인정보 보호법제 연구, 2017년 개인정보보호위원회 연구용역보고서.
[31] 이원태(2016), EU의 알고리즘 규제 이슈와 정책적 시사점, KISDI Premium Report

16-12호, 정보통신정책연구원.
[32] 이은우 외(2017a), 데이터 연계/결합 지원제도 도입방안 연구, 개인정보보호위원회 연구 용역보고서.
[33] 이은우 외(2017b), 빅데이터 활용과 개인정보보호 균형을 위한 개인정보보호법 개선 연구, 국회 행정안전위원회 연구보고서.
[34] 이은우 외(2018), EU GDPR 등 개인정보보호 규범 및 감독기구의 국제표준 확립 필요성 연구 - 국제규범의 변화와 국내 개인정보 보호체계 효율화 방안 연구, 개인정보보호위원회 연구용역보고서.
[35] 이인호 외(2017), 한국의 개인정보보호 수행체계 발전방안 연구, 개인정보보호위원회 연구용역보고서.
[36] 이정은(2019), EU 일반개인정보보호법(GDPR)에 대한 일본정부의 대응 및 평가.
[37] 전승재, 권헌영(2019), 개인정보 수집, 이용, 제3자 제공에 관한 4개국 법제 비교분석, 선진상사법률연구 통권 제85호.
[38] 채형복(2013). EU 기본권청. 동아법학.
[39] 최경진(2017), 4차 산업혁명 시대의 개인정보보호법제 개선방안, 법제연구 제53호.
[40] 한국인터넷진흥원(2018), 미국 캘리포니아 주 「소비자 프라이버시법」(The California Consumer Privacy Act of 2018) 주요내용 분석.
[41] 한국인터넷진흥원(2019), 유럽사법재판소의 프라이버시 쉴드 무효 판결 분석.
[42] 한국인터넷진흥원(2020), 우리 기업을 위한 2020 EU일반개인정보보호법(GDPR) 가이드북.
[43] 행정안전부(2016), 개인정보 비식별 조치 가이드라인- 비식별 조치 기준 및 지원·관리체계 안내-.
[44] 행정안전부(2016), 개인정보보호법령 및 지침·고시 해설.
[45] Fred H. Cate & Rachel Dockery, 김태오 옮김(2018), “인공지능과 개인정보보호 : 불필요한 갈등 증가에 대한 관견(管見)”, 경제규제와 법 제11권 제2호, 서울대학교 공익산업법센터.

2. 국외자료

[1] Access Now(2016), ACCESS NOW POSITION PAPER: UNDERSTANDING THE "RIGHT TO BE FORGOTTEN" GLOBALLY.

[2] Access Now(2019), EU Court decides on two major "right to be forgotten" cases: there are no winners here.

[3] Access Now(2020), TWO YEARS UNDER THE EU GDPR.

[4] Amit Datta et al(2018), Discrimination in Online Advertising A Multidisciplinary Inquiry, Proceedings of Machine Learning Research.

[5] ARTICLE 29 DATA PROTECTION WORKING PARTY(2010a), Opinion 1/2010 on the concepts of controller and processor adopted on 16 February 2010, WP 169.

[6] ARTICLE 29 DATA PROTECTION WORKING PARTY(2010b), Opinion 3/2010 on the principle of accountability adopted on 13 July 2010, WP 173.

[7] ARTICLE 29 DATA PROTECTION WORKING PARTY(2011), Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

[8] ARTICLE 29 DATA PROTECTION WORKING PARTY(2013), Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203.

[9] ARTICLE 29 DATA PROTECTION WORKING PARTY(2014a), Opinion 8/2014 on the on Recent Developments on the Internet of Things, 14/EN WP 223.

[10] ARTICLE 29 DATA PROTECTION WORKING PARTY(2014b), Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12, WP 225.

[11] ARTICLE 29 DATA PROTECTION WORKING PARTY(2017a), Guidelines on the right to data portability, 16/EN WP 242 rev.01, Adopted on 13 December 2016, As last Revised and adopted on 5 April 2017.

[12] ARTICLE 29 DATA PROTECTION WORKING PARTY(2017b), Guidelines on Data

Protection Impact Assessment and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. wp248rev.01. Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017.

[13] ARTICLE 29 DATA PROTECTION WORKING PARTY(2017c), Guidelines on Data Protection Officers (‘DPOs’), WP 243 rev.01. Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017.

[14] ARTICLE 29 DATA PROTECTION WORKING PARTY(2018a), Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679(17/EN, WP251, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018.

[15] ARTICLE 29 DATA PROTECTION WORKING PARTY(2018b), Guidelines on consent under Regulation 2016/679, 17/EN WP259 rev.01. Adopted on 28 November 2017, As last Revised and Adopted on 10 April 2018.

[16] Australian Human Rights Commission(2019), Human Rights and Technology : DISCUSSION PAPER.

[17] Barnard-Wills, David and Wright, David(2014), PHAEDRA : Improving Practical and Helpful co-operAtion bEtween Data pRotection Authorities.

[18] Brave(2020), Europe’s governments are failing the GDPR - Brave’s 2020 report on the enforcement capacity of data protection authorities.

[19] Committee on Standards in Public Life(2020), Artificial Intelligence and Public Standards.

[20] Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence(MSI-AUT)(2019), Addressing the impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems

[21] Council of Europe Commissioner for Human Rights(2019), Unboxing artificial intelligence: 10 steps to protect human rights.

[22] Court of Justice of the European Union(2016), PRESS RELEASE No 91/20, The

Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield.

[23] David Freeman Engstrom, Daniel E. Ho, Catherine M. Sharkey, Mariano-Florentino Cuéllar(2020), Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies.

[24] David Kay(2018), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348.

[25] EDPB(2020), Contribution of the EDPB to the evaluation of the GDPR under Article 97.

[26] EDPB(2020) Guidelines 07/2020 on the concepts of controller and processor in the GDPR(Version 1.0), Adopted on 02 September 2020.

[27] EDPS(2005), Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, 2005. 11. 28.

[28] EDPS(2011), Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

[29] EDPS(2012), Opinion of the European Data Protection Supervisor on the data protection reform package.

[30] EDPS(2015), Meeting the Challenges of Big Data: A call for transparency, user control, data protection by design and accountability Opinion.

[31] EDPS(2018), Position paper on the role of Data Protection Officers of the EU institutions and bodies, 2018. 9. 30.

[32] EDPS(2019), EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, Adopted on 07 November 2019.

[33] EDPS(2020), A Preliminary Opinion on data protection and scientific research.

[34] European Commission(2016), Guide to the EU-U.S. Privacy Shield.

[35] European Commission(2020), COMMUNICATION FROM THE COMMISSION TO THE

EUROPEAN PARLIAMENT AND THE COUNCIL - Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 2020.6.24 COM(2020) 264 final.

[36] European Union Agency for Fundamental Rights(FRA)(2010a), National Human Rights Institutions in the EU Member States, Strengthening the fundamental rights architecture in the EU I.

[37] European Union Agency for Fundamental Rights(FRA)(2010b), Data Protection in the European Union: the role of National Data Protection Authorities: Strengthening the fundamental rights architecture in the EU II.

[38] European Union Agency for Fundamental Rights(FRA)(2011), FRA opinion on the proposal for a Passenger Name Record (PNR) Directive.

[39] European Union Agency for Fundamental Rights(FRA)(2012). Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package.

[40] European Union Agency for Fundamental Rights(FRA)(2013), Access to data protection remedies in EU Member States.

[41] European Union Agency for Fundamental Rights(FRA)(2018a), Handbook on European data protection law - 2018 edition.

[42] European Union Agency for Fundamental Rights(FRA)(2018b), Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union - Volume II - Summary.

[44] European Union Agency for Fundamental Rights(FRA)(2018c). Fundamental rights implications of storing biometric data in identity documents and residence cards.

[44] European Union Agency for Fundamental Rights(FRA)(2018d), In Brief - Big data, algorithms and discrimination.

[45] European Union Agency for Fundamental Rights(FRA)(2018e), Preventing unlawful profiling today and in the future: a guide.

[46] European Union Agency for Fundamental Rights(FRA)(2019a), Facial recognition technology: fundamental rights considerations in the context of law enforcement.
[47] European Union Agency for Fundamental Rights(FRA)(2019b), The General Data Protection Regulation – one year on.
[48] European Union Agency for Fundamental Rights(FRA)(2020a), Your rights matter: Data protection and privacy – Fundamental Rights Survey.
[49] European Union Agency for Fundamental Rights(FRA)(2020b), Fundamental rights implications of COVID-19.
[50] European Union Agency for Fundamental Rights(FRA)(2020c), EU rights and data protection bodies: new technology and data protection have to go hand in hand, 2020.6.22.,
[51] European Union Agency for Fundamental Rights(FRA)(2020d), Strong and Effective national Human Rights Institutions: Challenges, Promising Practices and Opportunities.
[52] FTC(2012), Protecting Consumer Privacy in an Era of Rapid Change.
[53] Gabel, Detlev and Hickman, Tim(2016), "Chapter 14: Data Protection Authorities" in Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law. White & Case LLP.
[54] Global Partners Digital, Global Digital Policy Incubator(2020), National Artificial Intelligence Strategies and Human Rights: A Review
[55] Graham Greenleaf(2018), Questioning 'adequacy' (Pt II) – South Korea.
[56] ICDPPC(2018), Declaration on Ethics and Data Protection in Artificial Intelligence.
[57] ICO(2020), COVID-19 Contact tracing: data protection expectations on app development.
[58] INFORM(2018), D2.5 Review report on Directive (EU) 2016/680 aimed at the legal practitioners. Ref. Ares(2018)3815178.
[59] International Conference of Data Protection and Privacy Commissioners(2018), Declaration on Ethics and Data Protection in Artificial Intelligence
[60] Network of Data Protection Officers of the EU institutions and bodies(2010),

Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001, 2010. 10. 14.

[61] New Zealand Human Rights Commission(2018), Privacy, Data and Technology: Human Rights Challenges in the Digital Age.

[62] OECD(2013), The OECD Privacy Framework.

[63] OHCHR(2014), The Right to Privacy in the Digital Age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37. 2014.6.30

[64] OHCHR(2018), Artificial Intelligence Technologies and Freedom of Expression: A human rights approach to Artificial Intelligence (AI).

[65] OHCHR(2020), Report of the proceedings of the online expert seminar

[66] OPC(2020), Consultation on the OPC's Proposals for ensuring appropriate regulation of artificial intelligence.

[67] Peter J. Hustinx(2013), Interaction Between Data Protection Authorities and National Human Rights Institutions, in the National human rights institutions in Europe : Comparative, European and International Perspectives.

[68] Robert Madge(2017), GDPR: data portability is a false promise.

[69] Schutz, Philip(2012), Comparing formal independence of data protection authorities in selected EU Member States, Conference Paper, ECPR Standing Group on Regulation & Governance (Biennial Conference) <4, 2012, Exeter>.

[70] Scottish Human Rights Commission(2020), COVID - 19: Human Rights implications of digital contact tracing technology.

[71] UN(1990), Guidelines for the Regulation of Computerized Personal Data Files, Adopted by General Assembly resolution 45/95 of 14 December 1990.

[72] UN(2014), The right to privacy in the digital age, A/RES/68/167. Resolution adopted by the General Assembly on 18 December 2013, 2014.1.21.

[73] UN(2015), The right to privacy in the digital age, Resolution adopted by the General Assembly on 18 December 2014, A/RES/69/166. 2015.1.10

[74] UN(2017), The right to privacy in the digital age, Resolution adopted by the

General Assembly on 19 December 2016, A/RES/71/199. 2017.1.25

[75] UN Human Rights Council (2017), The right to privacy in the digital age. A/HRC/34/L.7/Rev.1.

[76] VentureBeat(2020), Stanford and NYU: Only 15% of AI federal agencies use is highly sophisticated.

[77] White House(2012), Consumer Data Privacy in a Networked World – A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.

[78] White House(2016), Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights.

유럽연합「개인정보보호 규정」(GDPR) 등
국제인권기준에 따른
개인정보 보호 법제도 개선방안 연구

| 인쇄일 | 2020년 11월
| 발행일 | 2020년 11월
| 발행처 | 국가인권위원회
| 주　소 | 04551 서울시 중구 삼일대로 340 나라키움 저동빌딩
http://www.humanrights.go.kr
| 연구기관 | 사단법인 정보인권연구소

ISBN : 978-89-6114-789-7 93360　비매품

ISBN : 978-89-6114-789-7 93360