개인정보보호법 정비방안 연구

A Study of Improving the Personal Data Protection Act

2012.12

한국인터넷법학회

제 출 문

개인정보보호위원회 위원장 귀하

본 보고서를 **『개인정보보호법 정비방안 연구』**의 연구결과 보고서로 제출합니다.

2012. 12

연 구 기 관 : 동국대학교

총괄책임자 : 김 상 겸 (동국대학교)

참여연구원 : 정 필 운 (교원대학교)

김 성 준 (법무법인 명율)

정 상 우 (인하대학교)

문 재 태 (동국대학교)

김 대 규 (한국외국어대학교)

목 차

Ⅰ. 연구의 목적

제1절 연구 배경 및 필요성

우리나라 개인정보보호법은 1980년 OECD 개인정보 가이드라인과 1995년 EU 개인정보지침을 모델로 한 세계에서 가장 최근에 제정된 개인정보보호에 관한 법률로써, 1995년 EU 개인정보보호지침, 일본 개인정보보호법, 기타 여러 나라의 개인정보보호법에 비해 진일보한 법이라는 평가를 받고 있다. 먼저 언급할 수 있는 것이 정보주체의 개인정보 자기결정권의 실질적 보장이다. 개인정보보호법은 어떤 정보들이 정보주체가 반드시 제공해야 할 필수정보이고, 어떤 정보들이 제공해도 되고 안 해도 되는 선택정보 인지를 명확히 구분하고 있다. 이렇게 구분해서 어떤 경우에도 정보주체에게 필수정보 이외의 개인정보 제공을 강요하지 못하도록 하는 것이 개인정보 최소수집원칙에 부합한 것이 된다. 그리고 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다. 즉, 최소정보(필수정보)의 입증책임 여부이다. 필요한 최소한의 개인정보는 거래내용, 거래방법, 서비스 수준, 서비스의 이행 방식, 결재수단 등 거래 환경에 따라 다르기 때문에 어떤 정보가 꼭 필요한 최소한의 개인정보인지는 해당 개인정보처리자가 가장 잘 알 수 있다. 따라서 개인정보처리자가 해당 개인정보가 필요한 최

소한의 개인정보라는 것을 입증하지 못하면 패소하게 된다. 다음으로 구분 동의의 의무화 등의 규정들을 두어 개인정보 피해예방 및 피해확산 방지를 위한 장치들을 마련하고 있는 것이다. 그리고 개인정보유출 사고 통지·신고제도, 개인정보 영향 평가제 등을 도입하여 개인정보 침해 시 피해를 위해서 신속한 구제수단을 마련한 점이다. 또한 개인정보 소송의 겨우 입증책임이 개인정보처리자에게 전환되어 있다고 하지만 정보주체가 공공기관이나 기업 혹은 단체를 상대로 소송을 진행한다는 것은 시간적으로나 비용적으로 감당하기 어렵다. 또 소송에서 이기더라도 승소액보다 소송비용이 더 많아 대다수 정보주체들이 권리행사 자체를 포기해 버리는 경우가 흔하다. 따라서 피해구제를 받는 데 소요되는 비용과 시간을 절감하면서도 소송절차에 준해서 공정하게 피해를 구제받을 수 있는 장치로써 개인정보분쟁조정제도, 집단분쟁조정제도 및 단체소송제도 등을 도입하였다.

그러나 개인정보보호법은 최근 EU, 미국 등에서 활발하게 논의되어 온 개인정보보호 이슈들에 대한 관심이 부족하고, 국제적 기준에 비추어볼 때 지나치게 규제적이며, 법 내용이 난해하고 불명확하다는 비판을 받고 있다.

첫째로 SNS, 클라우드 등의 환경에서 정보주체의 권리보호 방안이 미흡하다. 개인정보보호법은 수집과 처리의 목적을 달성하여 보존 필요성이 없어진 개인정보의 파기 의무를 규정하

는 한편, 정보주체에게 개인정보 처리정지 요구권과 삭제요구권을 붕하고 있지만 개인정보처리자 자신이 보유하고 있는 개인정보에 대해서만 파기와 삭제 의무를 부여하고 개인정보처리자가 제3자에게 제공하거나 공개한 개인정보에 대해서는 파기와 삭제 의무를 규정하고 있지 않고 있다. 대부분 개인정보처리자의 필요에 따라 계열사, 협력회사 등에게 개인정보가 제공·판매되고 있어 동의에 따른 결과와 책임을 모두 정보주체에게 지우는 것은 문제라고 할 수 있다. 즉. 정보주체의 잊혀질 권리(제3자에 대한 링크·복제 삭제요청 통지의무), right of data portability, Do-Not-Track, Privacy by Design, Privacy by Default, 개인정보 공개·공유원칙 등이 미반영 되어 있다. 둘째, 지나친 규제·처벌 위주의 규정으로 국제적 규범과 격차 발생이 발생하고 있다는 것이다. 매우 제한적인 수집·이용 기준, 목적 외 이용 기준, 제3자 제공 기준 및 영업의 자유를 과도하게 제한하는 위탁처리 절차·방법 및 변경 동의 의무, 중소기업에 대한 배려 부족 등을 들 수 있다. 그리고 형사 처분 위주의 과잉 처벌이라든지 불분명한 양벌규정의 경우도 생각해 볼 수 있다. 셋째, 다른 법령과 충돌·모순되거나 다의적 해석이 가능한 조문이 다수 존재한다. 일례로 '개인정보'에 관한 정의의 불명확, 최소한의 개인정보와 필수정보의 차이, 제18조 제2항 제5호의 절차·방법 및 효력, CCTV 설치, 운영 기준·절차, 스팸 메일과의 관계 등을 들 수 있다.

따라서 모바일 등 변화한 정보통신 기술 및 서비스 환경에서 정보주체의 권리를 보호하고, 규제의 합리화와 투명화를 통한 기업의 컴플라이언스 비용절감 및 국제 경쟁력 강화를 위하여 현행 개인정보보호법의 문제점과 개선방안을 비교법적인 관점과 법해석론적 관점에서 체계적으로 조사·분석할 필요가 있는 것이다.

제2절 연구의 목표

본 연구는 우리나라 개인정보보호법을 시행하면서 나타난 제반 문제점을 분석하여 그에 대한 구체적인 해결방안을 제시하는 것을 목표로 한다. 즉, 법 집행 과정에서 제기된 다양한 주장과 문제점을 분석한다. 이와 같은 목표 아래 본 연구보고서는 우리나라 개인정보보호법에 대하여 다음과 같은 문제의식을 가지고 출발할 것이다.

첫째, 최근 EU와 미국에서 논의되어 온 개인정보 이슈에 대한 이해 확대이다. 이러한 이슈 연구는 정부의 개인정보보호 정책 및 입법에 대한 방향성을 제시할 수 있을 것이다.

둘째, 모바일, SNS, 클라우드 등의 환경에서 정보주체의 권리 보호방안 마련으로, 정보주체의 개인정보 자기결정권 보장을 위한 구체적 수단 제공을 위한 방향성 제시이다.

셋째, 수집·이용·제공 기준 등의 합리화를 통한 국제기준과의 조화로서, 국내기업의 글로벌 경쟁력 강화, 해외기업의 국내 투자 촉진 등을 기대해 볼 수 있다.

넷째, 수범자가 이해하기 쉽고 예측 가능하도록 관련 법조항을 정비하여 기업의 컴플라이언스 비용절감 및 국제 경쟁력 강화를 위한 방향을 제시할 수 있다.

제3절 연구 범위 및 대상

1. 연구 범위

본 연구의 범위는 개인정보보호법 시행 과정에서 나타난 문제점 분석하는 것으로 다음과 같은 내용을 위주로 한다. 현행법의 미비점, 모순 사항, 보완 필요사항 등을 분석한다. 또한 개인정보보호법과 관련 다른 법률의 상충성·모순성 등 분석 및 법집행기관, 집행대상기관 등이 법집행과정에서 제기하는

문제점 등을 분석한다. 이러한 분석 하에서 개인정보보호법 개선방안 검토와 개선방향을 제시하고자 한다. 먼저 이슈별 현황 및 문제점, 개정 필요성, 개선방향 제시할 것이고, 국내·외 유사 입법례를 조사·분석하여 각국 개인정보보호법과 내용을 비교한 후 국내 법 개정에 따른 기대효과와 예상 문제점을 검토한다.

2. 연구 대상

본 연구의 주요 조사·분석 대상은 '개인정보보호법'으로 한정한다. 다만, 개인정보보호법과 다른 법률과 충돌·저촉·중복 등의 문제점을 분석하기 위해 필요한 범위 내에서 정보통신망법, 신용정보법, 위칙정보법 등도 검토의 대상으로 한다. 조사대상 해외의 법령 및 정책은 1995년 EU Personal Data Protection Directive, 2002년 ePrivacy Directive(2009년 개정), 2012년 EU General Data Protection Regulation, 독일, 영국, 일본 등의 대표적 해외법률과 OECD, APEC 등의 국제기구 최근 개인정보 이슈들이다.

Ⅱ. 주요국의 개인정보보호법 제·개정 현황

제1절 주요국의 개인정보보호법제의 개관

1. 고찰의 필요성

첫째, 주요국의 개인정보보호법의 체계와 내용을 고찰하는 것은 우리법제의 체계와 내용을 이해를 심화하고, 이를 보완하는데 시사점을 가져다 줄 수 있다.[1] 둘째, 국제화되고 네트워크로 연결된 사회에서 각 국은 자국 국민의 개인정보를 보호하기 위하여 개인정보의 국외이전을 제한하고 있는데, 이러한 제한의 주요기준이 자국과 이전국의 개인정보보호수준이다. 그러므로 세계 각 국은 자국 기업의 원활한 영업을 위하여 타국의 개인정보보호수준에 관한 동향을 살펴야 한다.[2]

2. 주요국의 입법특징 및 법제의 개관

유럽연합(EU)와 미국은 다음 몇 가지 면에서 개인정보보호 입법에 있어서 차이가 있다. 첫째, EU와 미국은 개인정보를

---

1) Daniel J. Solove, Marc Rotenberg, Paul M. Schwartz, Information Privacy Law, Aspen, p.869 참고.
2) op. cit, pp.929-930.

대하는 관점에 있어서 차이가 있다. EU는 개인정보를 정보주체 자신이 처분하는데 한계가 있는 권리로 바라보는데 반해서, 미국은 개인정보를 정보주체 자신이 전적으로 처분할 수 있는 권리로 바라본다. 둘째, EU의 개인정보보호법제는 '옴니버스(omnibus)'식인데 반해서, 미국의 개인정보보호법제는 '분절적(sectoral)'이다. 즉 EU의 개인정보보호법제는 전통적으로 공공영역과 민간영역의 일련의 개인정보보호 처리절차를 하나의 법에서 다룬다. 반면 미국의 개인정보보호법제는 생활영역별, 기술별로 개별법을 제정하여 규율하고 있다.[3)]

국제적으로 보았을 때, EU와 미국을 제외한 제3국가에서는 EU 개인정보보호법제를 모델로 하여 공공영역과 민간영역의 일련의 개인정보보호 처리절차를 하나의 법에서 규정하는 방향으로 입법화하는 것이 추세이다.[4)]

유럽의 개인정보보호법제는 유럽위원회의 전통적인 역할과 유럽연합의 부상하는 역할을 통하여 형성되어 왔다. 그것의 기원은 전후 유럽에서 인권 보호를 위하여 제정된 1950년 유럽위원회 협약(the Council of Europe Convention of 1950) 제8조이다. 그리고 협약 제8조는 유럽인권법원(European Court of Human Rights)의 판결과 1980년 개인정보보호협약에 의하여

---

3) op. cit, p.869. 이에 관해서 좀 더 자세한 것은 Joel Reidenberg, Setting Standards for Fair Information Practice in the U.S. Privacy Sector, 80 Iowa L. Rev. 497. 500 (1995)

4) Daniel J. Solove, Marc Rotenberg, Paul M. Schwartz, op. cit, p.869-870.

구체적인 효력을 발휘하였다.[5]

그러나 협약 제8조와 유럽인권법원의 판결, 1980년 개인정보보호협약의 중요성에도 불구하고, 유럽 개인정보보호법제는 「1995년 유럽연합 개인정보보호지침(the Data Protection Directive of the European Union)」[6]을 통하여 그 중요내용을 형성하였다. 이 지침은 유럽연합 회원국 뿐 아니라 전 세계 개인정보보호법제의 근본적인 발전을 가져오는 원동력이 되었다.

한편, 유럽연합에서는 발전하는 정보환경에 적합한 개인정보보호법제를 마련하기 위하여 최근 이러한 지침(directive)이 아닌 규정(regulation)의 형태로 법의 형식을 격상하고 이른바 '잊혀 질 권리'를 도입하는 등 보호 법제를 강화하는 것을 내용으로 하는 「2012 개인정보보호규정(Personal Data Regulation)안」[7]을 발표한 바 있다. 이미 살펴본 것처럼, 미국은 전통적으로 생활영역별, 기술별로 개별법을 제정하여 개인정보보호를 하여왔다. 그런데, 2012년 2월 23일, 1970년대 이래 사실상 '모델 프라이버시법'으로 역할을 해온 「공정 정보

5) 이상 op. cit. p.870.

6) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O. J. (L281) 0031-0050. 정보보호지침은 1995년 12월 13일 발효하였다.

7) REGULATION 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.

관행 규약(Code of Fair Information Practices, FIPPs)」을 최근의 IT환경에 적합하도록 대폭 보완한 「소비자 정보 프라이버시 보호 정책」(일명 소비자 프라이버시 권리장전)[8]을 발표하였으며, 연방공정거래위원회(Federal Trade Commission: FTC)도 2012년 3월 26일 「기업과 정책 담당자를 위한 소비자 프라이버시 보호 권고」[9]를 발표하였다.

아래에서는 이러한 EU와 미국의 개인정보보호법제에 대하여 고찰한다.

제2절 유럽연합

1. EU 개인정보보호지침

(1) 의의

1995년 10월 유럽연합의 개인정보보호지침이 채택되었다. 그러나 개인정보보호지침의 채택 이전에도 EU 회원국들은 각국

8) Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.

9) Protecting Consumer Privacy in an Era of Rapid Change : Recommendations for Business and Policymakers.

에서 개인정보의 보호를 위한 법제도를 가지고 있었다. 그런데 이들 관련 국내법규범은 개인정보의 보호라는 공통의 목적을 가지고 있었지만, 각 국가의 사정과 전통에 따라 다소 차이점을 가지고 있었다. 이러한 차이는 EU 회원국들 사이에서 정보의 자유로운 이전을 제한하게 되었고, EU의 공동시장(common market) 발전에 장애요인이 되었다. 예컨대, 개인정보가 회원국들 사이에서 이전되기 위하여 해당 회원국들 정보보호당국의 등록 또는 허가가 요구되었고, 각 회원국마다 서로 다른 기준이 적용되었다. 또한 일부 회원국은 개인정보 보호에 관한 법을 가지고 있지도 않았다. 이러한 현실에서 EU차원의 통일된 개인정보의 보호를 위한 입법이 요구되었고, 결국 정보보호지침이 채택된 것이다.

개인정보보호의 권리는 EU의 기본권헌장 (Charter of Fundamental Rights)의 제8조에 명시되어 있고,[10] 리스본조약으로 개정된 'EU기능조약' (Treaty on the Functioning of the European Union)의 제16조는 EU법의 모든 활동에서 개인정보보호의 법적 근거를 규정한다.[11] 2005년으로 채택 된지 10년이 된 정보보호지침은 개인의 정보보호에 있어 세계에서 가장 엄격한 법규범으로 인정되고 있다. 정보보호지침은 EU에 소재한 개인정보에 대하여 수행된 활동에 적용된다.

---

10) "Everyone has the right to the protection of personal data concerning him or her."

11) "Everyone has the right to the protection of personal data concerning them."

정보보호지침의 주된 목적은 크게 다음의 두 가지로 나누어 볼 수 있는데, 먼저 개인정보의 가공에 있어 해당 개인을 보호하며, 다음으로 EU내에서 각 회원국 국내법의 조화를 통한 개인정보의 자유이동을 보장하는 것이다.[12] EU의 정보보호지침은 일종의 골격규범으로서 각 회원국은 자신의 국내법제도를 통하여 동 지침이 달성하고자 하는 목적, 즉 EU회원국들에서 개인정보의 동일한 보호수준을 보장하는 목적을 1998년 10월 24일까지 이행하여야 하였다.[13]

EU법상 EU회원국은 지침 (directive)을 동 지침에서 규정된 일자 내에 국내법제도에 따라 이행하여야 한다. 지침이 EU회원국에서 법적 효력을 가지기 위하여 해당 회원국의 입법조치가 필요하지만, 이들 회원국의 입법조치는 해당 지침의 목적과 내용을 벗어날 수 없다. EU개인정보보호지침은 27개 EU회원국들은 물론 아이슬란드(Iceland), 리히텐슈타인(Lichtenstein) 및 노르웨이 등 EU회원국이 아닌 3개국도 본 지침을 택하기도 하였다.

EU 개인정보보호지침은 1998년 10월 24일까지 이행되도록 규정되어 있지만, 오직 스웨덴만이 이행일자를 준수하였다. 결국 동 지침의 이행일자는 2001년 10월 24일로 연기되었고, 영

12) 정보보호지침 제1조.
13) 박노형, “EU 및 영국의 개인정보보호법제 연구”, 법제처 연구용역보고서, 2010, 법제처, 20쪽.

국의 경우는 2000년 3월 1일 발효한 개인정보보호법 (Data Protection Act 1998: DPA)에 따라 동 지침을 이행하였다.

EU개인정보보호지침의 적용범위는 매우 넓다. 동 지침은 온라인이거나 오프라인 및 자동적이거나 수작업이 필요한 여부를 불문한 개인정보의 모든 처리에 적용된다.[14] 예컨대 소비자의 컴퓨터 데이터베이스는 물론 소비자의 이름 순서대로 정리한 카드파일도 정보보호지침의 적용을 받는다. 또한 개인정보보호지침은 개인정보를 보유한 모든 기관에 적용된다.

또한, 개인정보보호지침은 기술적으로 중립적이다. 즉, 동 지침은 개인정보의 처리에 사용된 기술적 수단에 상관없이 적용된다. 예컨대, 인터넷상의 개인정보의 '들어나지 않는'(invisible) 수집도 동 지침의 적용 대상이다. 그러나 개인정보가 '들어나는' (visible) 방법으로 수집되는 경우에, 자신의 정보를 이전하는 개인은 이러한 이전에 대하여 동의를 하였다고 볼 수 있을 것이다. 물론 이러한 개인은 관련 위험에 대하여 적절하게 통보받았어야 한다.

(2) 주요내용

(가) 개인정보

14) 정보보호지침 제3.1조.

EU 개인정보보호지침은 전적으로 또는 부분적으로 자동화 수단 (automatic means)으로 처리되는 개인정보에 적용되고, 개인을 참조하여 구성되는 파일링시스템에 보유된 수작업 데이터에도 적용된다. 그러나 동 지침은 EU조약의 Titles V와 VI, 공공안전, 국방, 국가안보 (개인정보의 처리가 회원국의 안보에 관련되는 경우 회원국의 경제복지를 포함), 및 형사법 분야의 회원국 활동에는 적용되지 않는다. 동 지침은 가사활동에도 적용되지 않는다. [15]

(나) 개인정보 처리의 조건

EU 개인정보보호지침의 제6조는 개인정보가 처리될 때 준수되어야 하는 기본원칙을 규정한다. 이들 원칙은 1984년 정보보호법의 규정과 유사하지만, 적용범위는 더 크다.[16] 제7조는 개인정보가 처리될 수 있기 전에 충족되어야 할 많은 조건을 규정한다. 정보주체의 동의에 의하여만 처리되어야 하는데 다음과 같이 처리가 필요한 경우는 예외이다: 첫째, 정보주체가 당사자인 계약의 이행에 필요한 경우; 둘째, 법적 의무를 준수하기 위한 경우; 셋째, 정보주체의 핵심적 이익을 보호하기 위한 경우; 넷째, 공공이익을 위하여 또는 공적권한의 행사에서 수

15) 박노형, 위의 연구보고서, 22-23면.
16) Peter Carey, Data Protection: A Practical Guide to UK and EU Law , 2009, p.7.

행되는 직무를 이행하기 위한 경우; 다섯째, 정보관리자의 정당한 이익을 충족하기 위한 경우로서, 정보주체의 이익 또는 기본권과 자유가 이러한 이익에 우선하는 경우는 예외로 한다.

(다) 개인의 민감정보

사람의 일정한 민족 또는 인종적 기원, 정치적 의견, 종교적 또는 철학적 믿음, 노동조합 회원자격, 건강 또는 성생활에 관한 정보를 드러내는 데이터의 특별범주 및 법의 위반과 유죄판결에 관한 데이터는 일정한 엄격한 조건에서만 처리될 수 있다. EU 개인정보보호지침의 제8조는 민감한 개인정보의 처리에 대하여 정보주체의 명백한 동의를 요구한다. 단, 회원국 법이 민감한 정보의 처리의 금지가 동의를 주는 정보주체에 의하여 해제될 수 없다고 규정한 경우는 예외로 한다고 규정하고 있다.

(라) 적법한 수집

EU 개인정보보호지침의 제10조는 개인정보가 정보주체나 제3자로부터 수집되는 경우, 정보주체는 정보관리자의 신원, 개인정보가 사용되는 목적, 및 공정한 처리를 보장하는데 필요한 추가적 정보를 제공받을 것을 규정한다.

(마) 정보주체의 권리

EU 개인정보보호지침이 규정한 정보주체의 권리는 다음과 같다. 제12조에 따라, 정보주체는 합리적인 간격으로 제약 없이 및 지나친 지연이나 비용 없이 개인정보에 대한 접근의 권리를 가지고, 또한 완전하지 않거나 정확하지 않은 데이터를 교정, 삭제 또는 차단하게 할 권리를 가진다. 제14조에 따라, 정보주체는 개인정보의 처리에 반대할 권리를 가지며, 정당한 경우 처리를 중단시킬 수 있고, 또한 직접 마케팅의 목적으로 사용되는 개인정보에 반대할 권리를 가진다. 제15조에 따라, 정보주체는 데이터의 자동적 처리에만 의존하고 법적 효과를 가지는 결정에 복종하지 않을 권리를 가진다. 다만, 동 결정이 결과가 정보주체에게 부정적으로 영향을 주지 않는 계약에 연계되지 않아야 하고, 법으로 허가되지 않아야 한다. 이 경우 정보주체의 이익이 보장되어야 한다.

(바) 보안

EU 개인정보보호지침의 제17조는 개인정보가 우연하거나 불법적 파괴네 우연적 손실로부터 보호되도록 데이터의 안전이 보장될 것을 요구한다. 또한, 데이터는 허가받지 않은 수정, 공개 또는 접근 및 다른 모든 형식의 불법적 처리로부터 보호되어야 한다. 안전 수준은 개인정보의 처리로 야기되는 위험과

보호되어야 하는 데이터의 성격에 적절하여야 하고, 기술 수준과 비용이 고려되어야 한다.

(사) 책임

EU개인정보보호지침의 제23조는 개인정보의 불법적인 처리 운용이나 동 지침에 따라 채택된 국내규정에 위반되는 행위로 발생한 손해에 대하여 정보 관리자에게 배상책임을 규정한다.

(아) 외국으로의 이전

EU 개인정보보호지침의 제25조는 처리되고 있거나 처리가 의도된 개인정보가 유럽경제지역 (European Economic Area: EEA)[17] 역외로 이전될 수 있는 조건을 규정한다. 일반적으로 제3국이 정보주체의 권리와 자유의 적절한 보호 수준을 보장하는 경우에 개인정보가 이전될 수 있다. 그러나 정보주체가 동의를 주거나 이전이 계약의 이행이나 공공이익의 차원에서 법적으로 요구되는 경우에는 예외가 인정된다.

---

17) 유럽자유무역지역 (European Free Trade Area: EFTA)을 구성하는 노르웨이, 아이슬란드 및 리히텐슈타인이 유럽연합의 내부시장에 참여할 수 있도록 1993년 3월 17일 채택되고 1994년 1월 1일 발효한 EEA협정 (Agreement on the European Economic Area)에 따라 EEA가 수립되었다.EFTA의 또 다른 구성국인 스위스는 EU와 별도의 양자조약을 체결하였다. http://www.efta.int/eea/eea-agreement.aspx <최종방문 12.09.30>

(자) 개인정보보호당국

EU 개인정보보호지침의 제28조는 각 회원국이 자국 내에서 동 지침을 이행하는 국내법의 적용을 감독할 감독당국을 설치하도록 요구한다. 컴퓨터에 의한 개인정보의 처리는 감독당국에 통지되고 등록되어야 한다. 일정한 경우에 통지요건의 면제 또는 단순화가 인정된다.

2. EU 개인정보보호규정안

(1) 추진배경

유럽위원회는 디지털 환경에서 개인의 개인정보 보호를 강화하면서 개인정보의 자유이전을 보장하기 위하여 2010년 11월 4일 1995년 EU 개인정보보호지침의 개정을 위한 전략을 발표하고, 지침에 대한 개정방안을 제출하였는데, 그 특징은 다음과 같다. 첫째, 개인정보의 수집과 사용이 최소한의 필요에 따르도록 개인의 권리가 강화된다. 둘째, 기업의 행정적 부담을 경감하여 개인정보의 원활한 자유이전을 보장하기 위하여 단일시장(single market) 차원이 제고된다. 셋째, 개인의 개인정보가 경찰과 형사정의 분야에서도 보호되도록 이들 분야에서의 개인정보보호에 관한 규범이 개선된다. 이와 관련하여 유럽위원회는 6개월에서 2년의 기간 동안 트래픽데이터 (traffic

data)를 보관하도록 요구하는 2006년 데이터보유지침(Data Retention Directive)을 검토하고 있다. 넷째, EU역외로 개인정보 이전의 절차를 개선하고 간소화하여 역외로 이전된 개인정보 보호수준을 제고한다. 다섯째, 정보보호당국의 권한과 역할을 강화하고 조화하여 개인정보보호 관련 규범이 보다 효과적으로 집행하는 안을 우선적으로 마련하였다.

이후 유럽위원회는, 여러 회의를 거쳐 2012년 1월 25일 유럽집행위원회(European Commission)은 온라인에서 개인정보를 더욱 보호하고, 디지털경제를 촉진하기 위하여 현행 개인정보보호규범을 포괄적으로 변경하는 「개인정보보호규정(General Data Protection Regulation)」을 입법예고 하였다.

그 주요 이유는 우선, 앞서 설명한 내용처럼 1995년의 개인정보보호지침은 강제성을 갖지 않기 때문에 스웨덴을 제외한 대부분의 국가는 이행기를 지키지 아니하였다는 문제가 발생하였고, 이러한 규범체계가 각 국에 따라 개인정보보호 수준과 집행기관이 상이한 이유로 하나의 EU 시장을 만드는데 큰 걸림돌로 작용하게 되었기 때문이다. 이에 따라 각 회원국의 이행입법 없이, 직접 회원국을 구속하는 규정(Regulation) 형태의 개인정보보호법안을 마련하여 위와 같은 걸림돌을 제거하기 위한 내용을 규정하고, 각 국의 사정을 고려하여야 하는 내용은 이와 별도로 기존의 1995년 개인정보보호지침의 개정안에 규정하여 입법예고를 하게 된 것이다.

(2) 주요 내용

(가) 개인정보관리기관 사전 등록제도 시행

개인정보보호법안 제3조에서는 개인정보관리 및 처리기관이 개인정보관리를 위해서는 반드시 사전에 동의를 취득하여야 적법하도록, Opt-In 방식을 채택하고 있다.

(나) 이른바 '잊혀 질 권리' 도입

개인정보보호법안 제15조에서는 자신의 정보가 불법적으로 인터넷에 공개된 경우, 해당 정보를 삭제하거나 추가로 공개하지 않도록 ISP에게 요구할 수 있는 이른바 '잊혀 질 권리'(right to be forgotten)를 인정하고 있다.

(다) 개인정보관리기관으로부터 제3자에게 이전할 수 있도록 요구할 수 있는 권리

개인정보보호법안 제16조에서는 자신의 정보를 저장장치에서 전자적으로 복제하여 얻을 수 있고, 개인정보관리기관으로부터 제3자에게 이전할 수 있도록 요구할 수 있는 권리(right of data portability)를 신설하였다.

제3절 미국

1. 전통적인 개인정보보호법제

(1) 개관

미국의 개인정보보호는 연방정부기관이 보유하고 있는 개인정보에 관한 보호법규인 1974년의 프라이버시법(Federal Privacy Act 1974)과 각 주단위로 규정된 프라이버시권 관련 법률들이 있다. 미국의 개인정보보호는 공공부문과 민간부문으로 나누어 공공부문에만 법을 적용하고 민간부문에는 원칙적으로 윤리적인 통제만 가능하게 되어 있다. 미국의 개인정보보호제도는 1966년의 정보공개법(Freedom of Information Act) 제정에 따라 연방정부가 보유하고 있는 정보를 원칙적으로 공개하되 프라이버시법에 의해 정부에 대한 규제를 가하고, 민간부문에는 정보의 자유로운 유통을 보장하며 개별 분야에서의 개인정보보호를 목적으로 한 영역별 보호 법제를 가지고 있다는 점이 특색이다.

미국에서는 1974년 프라이버시법이 제정된 아래 1978년 금융프라이버시권법, 1986년 전기통신보호법, 1988년 컴퓨터 자료의 상호 비교 및 프라이버시 보호법, 1994년 전기통신 프라이

버시법, 1996년 통신법 및 의료기록 비밀보호법이 각각 제정되었다. 한편 국가정보 통신기반 구축을 위해 정보통신기반 전담팀에 정보정책위원회를 구성하여 세 개의 팀 중 하나인 프라이버시 팀이 1995년 6월에 '프라이버시와 개인정보제공 및 이용의 원칙'을 작성했다. 동 원칙은 계약 자유에 따라 제공자의 통지와 소비자의 동의라는 두 개의 필수조건을 감안하면서 업계의 자율적인 규제가 우선이라는 것을 강조하고 있다.

미국의 개인정보보호법제의 특색인 영역별 방식에 따라 개인정보보호를 위한 많은 개별 법률이 제정되고 있는데 개별법의 장점은 특히 보호가 필요한 개인정보의 취급영역에 한정하여 법적 규제를 행하는 점이라고 하겠다. 그러나 단점으로는 개별 영역별로 법률을 제정하기 때문에 관련업계나 이익단체의 영향을 받을 수 있는 우려가 많다.

최근 미국은 프라이버시 보호를 강화하기 위한 한 방편으로 2002년 전자정부법에서 정부기관이 전자정부 사업을 추진하기 전에 반드시 당해 전자정부사업이 개인정보 및 프라이버시에 미치는 영향을 분석 및 평가하여 그 대책을 마련할 것을 의무화하는 프라이버시 영향평가제도를 명문화하였다. 이처럼 미국도 개인 프라이버시의 규제에 대한 중요성과 필요성을 인지하고 그에 맞게 빠르게 변화하고 있는 추세이다.

(2) 주요내용

미국에는 분야별로 약간의 차이가 있는 개인정보보호법이 존재한다. 첫째로 금융기관에 대한 내용을 살펴보면 금융기관이 보유하고 있는 개인정보에는 개인의 금융거래나 상거래와 관련된 정보뿐만 아니라 고객정보를 위시하여 각종 개인정보가 포함되어 있다. 따라서 그 정보가 누설되거나 제3자에게 함부로 공개되는 경우에는 개인의 경제활동에 관해 상세한 상황이 밝혀지게 됨으로 금융기관이 보유하고 있는 정보의 취급을 위해서는 세심한 주의가 필요하다. 미국에서는 이와 같은 이유로 금융기관의 고객정보가 법적 보호의 대상이 되는 개인정보로서 프라이버시의 권리에 기초하여 보장되고 있다.

금융 프라이버시법은 정부기관에 의한 금융기록의 접근을 원칙적으로 금지하고 예외적으로 고객의 동의, 행정기관의 소환영장, 수색영장, 사법기관에 의한 소환영장, 공식적인 서면청구에 의하지 않으면 정보는 공개되지 않는다. 또한, 금융기관의 개인정보 취급에 관해 금융기관의 보호정책을 명시할 의무를 부과하고 소비자가 스스로 개인정보의 이용에 관한 선택을 할 때 지침이 될 수 있는 정보를 제공하도록 규정했다. 아울러 소비자가 관련회사 이외의 제 3자와 정보공유를 선택할 수 있게 하기도 했다.

특히 의료정보에 있어서 개인정보의 경우, 미국에서는 의료분

야의 개인정보보호를 목적으로 하는 법률이 제정되지 않았지만 의료분야의 개인정보에는 정보주체가 되는 환자에 관해 일반적인 개인식별정보에 더하여 진료기록이나 유전자에 관한 정보 등의 매우 중요한 정보가 많이 포함되어 있는 경우가 흔하다. 이 때문에 의료분야의 개인정보를 다루지 않으면 안 되는 상황이 되었다.

최근 들어 의료분야의 개인정보보호에 적극적인 자세를 보여 1999년에는 유전자 정보 보호를 포함한 '신기술시대의 의료프라이버시 법률안(Medical Privacy in the Age of New Technologies Act of 1999)'이 제출되는 등 많은 의료정보에 대한 정보보호 활동이 이루어지고 있다. 이처럼 미국에서 의료분야의 개인정보를 엄격하게 보호하려는 것은 의료에 관한 여러 가지 기록에의 접근 및 그 보호의 문제가 중요할 뿐만 아니라 유전자에 관한 정보의 보호 등의 문제가 21세기에는 개인정보보호의 핵심적인 과제가 될 것으로 예상하고 있기 때문이다. 뿐만 아니라 미국에서는 개인의 시청경향에 관한 정보 케이블통신정책법(Cable Communication Policy Act of 1984), 보도기관의 개인정보보호를 위한 1980년의 프라이버시보호법' 등이 존재한다.

또한, 금융 업체들은 고객의 정보를 마케팅 목적으로 전송을 할 경우 반드시 opt-out 옵션을 제공해야 한다. 미국의 MPA는 우편 선호, e-메일 선호, 전화 선호 서비스에 대한 책임을

가지고 있으며 연방의 Do-Not-Call list는 근본적으로 opt-out으로 운영되고 만약 데이터 제공자가 opt-out의 옵션을 선택하였을 경우 7일 이내에 요청을 실행에 옮겨야 한다.

미국의 경우 민감하지 않은 데이터에 대한 특정 정의는 내리고 있지 않으나 유럽에서와 마찬가지로 민감한 정보에 대한 정의는 내리고 있다. 미국에서 정의하는 민감한 정보로는 종교, 인종, 정치, 성 관심, 건강, Trade Union Member로, 이에 해당하는 데이터를 수집, 또는 활용을 원할 경우 데이터 제공자의 동의는 필수적으로 필요하다. 또한, Federal Trade Commission(FTC)는 데이터를 안전하게 처리 및 유통하지 않는 웹사이트, 데이터베이스 등의 매체에 대해서는 Consumer Protection Law를 적용시킨다고 명시하고 있다. FTC는 이미 오프라인과 온라인의 데이터 활용에 대해 위반한 회사에 대해 규제를 행하였고 만약 웹사이트와 같은 매체에서 프라이버시 보호의 방침이 없을 경우 Unfair Commercial Practices의 범위 안에서 이를 처리한다.

2. 미국 오바마 정부의 소비자 프라이버시 권리장전

(1) 배경

오바마 정부는 2012년의 새로운 온라인 프라이버시에 대한 프레임워크를 발표하면서 그 배경을 “미국 소비자들은 그들의 개인정보가 안전하다는 확신을 줄 수 있는 명확한 룰을 더 이상 기다릴 수 없는 실정이고, 더불어 인터넷이 발전함에 따라, 소비자의 개인정보관리에 대한 신뢰는 디지털 경제의 지속적인 성장에 필수적이라 할 것”이라고 설명하며, 2012년 2월 23일 미국의 오바마 행정부가 2010년 발표된 상무성 소속 인터넷정책 TF의 그린페이퍼(Green Paper)에 기초하여, 세계 디지털 경제의 성장과 변화를 꾀하면서도 동시에 소비자의 프라이버시 보호를 개선시킬 수 있는 전면적 청사진으로서 ‘온라인 프라이버시의 프레임워크(Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy)’을 발표하게 되었다.

특히, 디지털시대에서의 신뢰유지는 온라인상의 경제활동을 보호하는 것이며, 특히 소비자들의 신뢰를 높이기 위해 기술적·관리적 차원에서 개인사생활의 보호가 매우 중요하다는 것을 천명하였다. 이는 오프라인을 기반으로 하는 시장 활동이 온라인 기반으로 전환이 되면서, 클라우드 컴퓨팅, 위치 기반 서비스 등을 중심으로 미국 경제활동의 패러다임이 전환이 되었고, 경제적 이익의 지속적인 유지를 위하여 소비자의 기술네트워크에 대한 신뢰확보가 중요한 과제로 부각된 것이다.

(2) 프레임워크의 네 가지 요소

오바마 정부의 소비자 권리장전의 프레임워크는 네 가지 요소로 이루어졌는데 (1) 소비자를 위한 온라인 프라이버시 권리장전의 제정, (2) 인터넷업체 그룹, 소비자 그룹 등의 다양한 이해관계인의 합의를 바탕으로 한 온라인 프라이버시 권리장전에 부합하는 실효적인 법규의 제정, (3) 미국 FTC(Federal Trade Commission)의 법집행 강화, (4) 정보장벽을 낮추기 위한 세계 여러 나라와의 프라이버시 기준의 상호 운용성 고려가 그것이며, 이 중의 핵심은 '온라인 프라이버시 권리장전'이다.

(3) 소비자 프라이버시 권리장전 7원칙

소비자 프라이버시 권리장전은 소비자의 7가지 권리를 보호하는 사항을 핵심적으로 규정하고 있는데, 내용은 다음과 같다.

(가) 자기정보통제권(Individual Control)

소비자는 자기 자신에 대한 정보의 권리 주체자로서, 개인정보 수집기관의 수집정보의 유형 및 이용방법 등에 관한 통제

권을 행사할 수 있다. 이에 대하여 기업은 개인정보의 권리자인 소비자가 쉽게 이용하고 접근할 수 있는 서비스를 제공하지만, 개인정보의 수집 및 이용에 관하여 소비자가 직접 선택할 수 있도록 지원하여야 한다.

최근에는 사생활 보호기능을 강화하는 “추적 금지(Do Not Track)[18]” 기술을 통하여 소비자가 자신의 개인정보를 통제할 수 있도록 지원하고 있다.

(나) 투명성(Transparency)

소비자는 개인정보보호 및 보안실무에 관한 정보를 알 권리가 있다. 또한 가장 적절한 시기와 적절한 장소에서, 소비자들은 사생활 침해위험과 관련된 의미 있는 정보를 제공받아 개인별 통제권을 행사할 수 있다.

이에 대하여 기업은 소비자가 수집하는 정보, 필요성, 이용방법, 삭제 등에 관한 설명을 제공하여야 하고, 사생활 보호관련 서비스의 소비자 접근을 높이기 위하여, 구독이 용이하고 효과적인 방법을 제공하여야 한다. 특히, 최근 스마트기기의 발달로 인하여 휴대기기를 사용하는 경우가 많기 때문에, 이러한 특성을 고려하여 휴대기기이용자를 위한 효과적인 정보의 구독방법을 제시하여야 한다.

18) 상세한 사항은 Ⅲ에서 살펴보고자 한다.

(다) 맥락의 존중(Respect for Context)

소비자는 기업의 개인정보의 수집・이용・공개과정에서 일관된 맥락에서 이루어지도록 기대할 권리가 있다. 기업은 소비자에게 사전 공지한 내용과 같은 방식으로 정보를 활용하되, 개인정보 공개를 최소화해야 하는 의무가 발생하게 된다.

만약, 기업이 개인정보를 목적 외로 이용하거나 공개할 경우 투명성 및 개인통제권의 침해로 간주하여 사건 발생 즉시 기업을 고발할 수 있다. 그렇기에 기업은 소비자의 나이와 교양 수준 등에 따라 적절한 방침을 적용하도록 의무를 다해야 하는 것이다.

(라) 정보보안(Security)

소비자는 자신의 개인정보가 안전하고 신뢰할 수 있는 수준의 보안이 이루어지도록 요구할 권리가 있다. 이에 대하여 기업은 개인정보의 무단접근・이용・파괴・수정・공개 등을 방지할 보안대책을 수립하여야 한다.

(마) 접근성 및 정확성 강화(Access and Accuracy)

소비자는 데이터의 민감도・위험도를 고려하여, 적절한 방법

과 이용 가능한 형태로 개인정보에 접근 및 수정을 할 수 있는 권리가 있다.

한편, 기업은 합리적인 방법을 통해 개인정보를 보유 및 관리할 의무가 발생한다. 기업은 소비자가 자신의 개인정보를 수정·삭제·제한을 요구할 때, 사전에 수집한 소비자의 개인정보에 대하여 접근할 수 있도록 해야 하며, 소비자가 자신의 개인정보에 대하여 접근·수정·삭제를 요구할 때, 가장 적절한 방법으로 개인정보를 취급하여야 한다.

(바) 최소수집의 원칙(Focused Collection)

소비자는 특정기업의 개인정보 수집 및 보유에 관하여 합리적 제한을 할 수 있다. 이에 대해서 기업은 소비자정보보호법하에 기업의 목적달성을 위한 최소한의 개인 정보를 수집하여야 하며, 목적달성한 개인정보는 안전하게 삭제하여야 한다.

(사) 책임성 강화(Accountability)

소비자는 기업이 소비자 개인정보인권선언을 준수하며, 소비자의 개인정보를 적절한 방법으로 처리하도록 할 권리가 있다. 이에 대하여 기업은 정부와 소비자가 해당개념의 권리를 시행할 수 있도록 할 의무가 발생한다. 기업은 직원이 해당개념의

책임이 있음을 숙지시켜야 하며, 이에 따른 개인정보 취급이 이루어지도록 교육하고 평가하여야 한다. 또한 개인정보침해사고의 발생시, “책임(Accountability)”의 개념에 따라 계약상의 의무를 다하지 못하였기 때문에 법적인 처벌을 받을 수 있다.

3. 연방거래위원회 개인정보보호를 위한 보고서

(1) 개요

미국 연방거래위원회(FTC)에서는 인터넷 상에서 방대한 양의 개인 정보를 자신도 모르게 노출하고 있는 인터넷 사용자들의 프라이버시를 보호하고자, 2012년 3월 26일 ‘급속한 변화의 시대에 맞춘 소비자 개인 정보 보호(protecting consumer privacy in an era of rapid change)’라는 제목의 보고서를 발간하였다. FTC는 이 보고서를 통하여 사업자가 이용자의 개인정보보호를 위해 적용해야 하는 구체적인 프레임워크 및 개인정보정책 마련에 필요한 권고안을 제시하고 있다.

(2) 주요내용

(가) 추적금지(Do-Not-Track) 옵션 제공을 강제

이 보고서에서는 “추적금지(Do-Not-Track: 이하 DNT) 옵션 제공을 명시하고 있다. 여기서 추적(Tracking)이란 인터넷 이용자의 행동 및 구독습관의 기록을 공간, 가상공간, 시간과 연결시킬 수 있는 정보를 습득행위를 말하는데, 이를 통해 소비자의 개인정보를 임의로 가공하여 사업자간의 일종의 상품으로서의 가치를 가질 수 있을 만큼, 개인정보의 중요성이 커져가고 있다. 이에 대해 미 정부는 인터넷 이용자와 사업자간의 수·발신 정보의 대응방법을 정책적으로 대응하기 위한 조항이라 할 수 있다.

추적금지 옵션 제공의 강제는 사용자들이 직접 개인정보 추적 수준을 제한할 수 있도록, 브라우저 벤더들(browser venders)들에게 추적 금지 옵션을 제공하도록 강제하는 조항이다. 추적금지 옵션은 이용자가 개인정보 수집을 거부할 선택권을 갖는 시스템이며 이용자가 자신의 개인정보 추적 수준을 제한할 수 있는데, 이에 대해 주요 기업(페이스북, 구글 등)들은 추적금지 버튼을 도입할 예정이다.

기술적인 측면을 살펴보면, 이용자가 컴퓨터 웹을 통해서 정보를 송수신할 때, 컴퓨터 요청문에는 헤더(header)라고 불리는 작은 정보를 가지게 되는데, 이 헤더에는 사용자가 이용하고 있는 웹브라우저, 사용자 컴퓨터의 언어설정, 그 외 기술적

세부정보들을 포함하고 있는 것이다. DNT는 이 헤더에 컴퓨터 언어로 “Do-Not-Track”이라는 의사표시의 내용을 포함하여, 이용자가 원할 경우 원클릭 버튼을 통하여 이용자 본인의 이용내역을 추적하지 않도록 하는 명령문을 실행하게 되는 것이다.

(나) 기업의 ‘Privacy by Design’ 도입 촉구

‘Privacy by Design’는 개인정보보호를 위해서 설계 단계부터 이용자의 프라이버시를 고려해야한다는 개념으로서, 개인정보보호를 위한 설계 단계에서 기업이 서비스·상품 성격 및 개인정보 주기를 반영한 취급방침을 마련하고, 개인정보 취급방침을 통해 개인정보 기술적 보호, 최소한의 정보 수집, 목적에 합당한 보유 기간 설정, 개인정보 파기 방침, 정보 정확성의 유지 등을 보장하도록 하고 있다.

(다) 이용자 선택권 강화

개인정보의 수집·수집 목적 외 이용·특정 목적을 위해 이용자의 민감정보를 수집할 경우에, 이용자의 동의를 구하여야 하고, 기업은 이용자에게 강요하는 것이 아닌 선택권을 보장해야한다는 내용을 담고 있다.

또한 행태정보를 수집하는 사업자는 III에서 설명한 “Do-Not-Track” 기술과 같은, 이용자가 정보수집 여부를 선택할 수 있는 시스템을 제공하여야 한다.

(라) 데이터 브로커의 규제

정보 수집에 대한 투명성 강화를 위해 '중앙 집권적으로 관리할 수 있는 웹사이트(Centralized Website)'를 만들어 데이터 브로커들의 정체를 공개하고 사용자의 개인 정보를 수집하는 방법 등에 대해 밝힐 것을 요구하였다. 또한 사용자 개개인이 데이터 브로커가 수집한 정보에 접근할 수 있도록 하여 줄 것을 의회에 요청하였다.

(마) 자율규제의 시행을 위한 코드(self-regulatory codes) 추진

보고서에서는 기업과 개인정보보호를 주장하는 시민단체가 자율규제 시행을 위한 기준을 마련할 것을 요구하고, 이것이 마련되면 FTC는 이것이 집행될 수 있도록 조력할 것을 촉구하였다.

(바) 개인정보 취급방침의 투명성 증진

기업은 이용자에게 개인정보의 취급방침을 고지함에 있어서, 명확하고, 간결해야하며 표준화가 되어 있어야 한다고 권고하고 있다. 특히 표준화에 대하여 FTC는 각 산업 분야 별 수집하는 정보 및 정보의 다양성을 인정은 하지만, 정보주체인 이용자가 명확한 이해를 위하여 미국 상무성 주도아래 개인정보 관련 용어 및 취급방침의 표준화에 대하여 논의를 진행하기로 하였다.

또한 개인정보 성격에 따른 차별적인 접근권을 보장하도록 하였다. 특히 FTC 보고서에서는 3가지형태로 나누어 설명하고 있는데, 먼저 상품 및 서비스를 제공하는 업체의 경우에는 이용자의 개인정보에 대해, 자신들이 수집하고 보관하고 있는 개인정보의 리스트를 공개하도록 하고 있다. 다음으로, 은행・보험・고용 등 업무적으로 이용하는 경우에는, 이용자에게 자기정보 접근 및 정정 요구권 등을 보장하도록 설명 하고 있다. 마지막으로 최근 급격하게 시장이 커진 SNS나 검색엔진 등의 경우에는, 사업자가 이용자에게 수집하는 정보의 종류 및 수집 경로를 공개하도록 권고하고 있다.

Ⅲ. 클라우드·빅데이터 환경에서 정보주체 권리강화

제1절 국외이전 개인정보의 보호 강화 (제14조)

1. 현황 및 문제점

최근 해외 기업들의 국내 투자와 국내 기업들의 해외 진출이 활발해 짐에 따라 우리나라 국민의 개인정보가 국외로 이전하는 현상이 일상화 되고 있다. 특히 본사를 해외에 두고 있는 다국적 기업이나 글로벌 IT기업의 경우 거의 대부분이 고객 개인정보를 보관·관리하고 있는 데이터센터를 해외에 두고 있어 국내 지점이나 자회사에서 수집·이용되는 고객 개인정보가 모두 해외로 이전·저장되고 있다. 향후 클라우드컴퓨팅 환경이 본격화되면 국내 소비자 정보의 해외 이전 현상은 더욱 가속화 될 것으로 예상된다.

그러나 개인정보보호법은 개인정보 국외 이전에 대하여 아무런 기준을 제시하지 않고 정보통신망법에만 의존하고 있다. 그런데 정보통신망법은 개인정보 국외 이전 시 정보주체의 동의를 받도록 되어 있고 이전되는 개인정보에 대하여 기술적·관리적 보호조치를 해야 한다고 규정하고 있으나 법 위반에 따른 행정처분이나 형사처분 규정은 없다.[19] 또한 동의를 받는다

고 해서 정보주체의 권리가 실질적으로 보호되는 것도 아니어서 형식적인 동의 절차만으로는 국외 이전 개인정보를 보호하는데 한계가 있다. 이로 인해 국경을 초월한 디지털 경제 환경에서 국내 소비자들의 개인정보보호가 방치되고 있는 현실이다.

한편 개인정보보호법은 개인정보를 '국외의 제3자에게 제공할 때'에는 정보주체에게 알리고 동의를 받아야 한다고 규정하고 있으나,[20] 이 규정만으로는 국외로 이전되는 국내 정보주체들의 권리를 보호할 수 없다. 동의만으로는 정보주체의 권리를 보호할 수 없거니와 동의의 대상도 제3자 제공으로 한정되어 있기 때문이다.

---

19) 제17조(개인정보의 제공) ③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

20) 제63조(국외 이전 개인정보의 보호) ① 정보통신서비스 제공자등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결하여서는 아니 된다.
② 정보통신서비스 제공자등은 이용자의 개인정보를 국외로 이전하려면 이용자의 동의를 받아야 한다.
③ 정보통신서비스 제공자등은 제2항에 따른 동의를 받으려면 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다.
1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 이전일시 및 이전방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간
④ 정보통신서비스 제공자등은 제2항에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다.

또한 국외 제3자 제공과 국외 이전은 구분하여야 한다. 국외 이전은 위탁의 경우도 있을 수 있고, 영업의 양도·양수에 따른 경우도 있을 수 있으므로 국외 제3자 제공보다는 훨씬 넓은 개념이다. 그런데 개인정보보호법 제17조 제3항은 국외의 제3자에게 개인정보를 제공할 때에는 정보주체의 동의를 받으라고만 되어 있어 모든 형태의 제3자 제공에 대해서 동의를 받으라는 것인지, 제3자 제공에 대하여 정보주체의 동의가 필요한 경우에만 국외의 제3자에게 제공된다는 사실을 특별히 알리고 동의를 받으라는 것인지가 불분명하다. 후자로 해석할 경우 개인정보보호법 제17조제3항에 따라 국외 제3자 제공에 대하여 동의를 받아야 할 대상은 더욱 좁아진다. 제17조제3항의 해석에 대하여는 다음 장(Ⅳ.2)에서 후술한다.

2. 개정방향

개인정보처리자가 개인정보를 국외로 이전하고자 하는 경우에는 미리 개인정보를 제공받는 국외의 제3자와 개인정보보호를 위한 기술적·관리적 조치, 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 사항, 그 밖에 이용자의 개인정보 보호를 위하여 필요한 조치 등이 포함된 정보보호계약을 체결하도록 하고, 필요한 경우 보호위원회는 상기 내용이 모두 포함된 표준 정보보호계약서를 작성하여 개인정보처리자에게 사용을 권

고할 수 있게 한다.

또한 보호위원회는 개인정보처리자 등의 요구가 있는 경우 개인정보를 이전받는 국가의 법령, 기술, 관행 등 전반적인 개인정보보호 수준을 검토·평가해서 해당 국가를 개인정보 이전 적합 국가로 지정·고시할 수 있게 함으로써, 이 경우에는 별도의 정보보호계약을 체결하지 않고도 개인정보를 이전받은 자가 해당 국가의 법령을 준수하는 것을 조건으로 개인정보를 국외로 이전할 수 있게 하는 것이 바람직하다.

유럽연합과 마찬가지로 보호위원회가 작성해서 권고하는 표준 정보보호계약서에 의하지 아니한 경우에는 보호위위원회 또는 행정안전부의 사전 승인을 받도록 하는 방법도 고려할 수 있으나 임의의 정보보호계약의 경우 제29조에 따른 기술적·관리적 조치 등을 모두 포함하도록 하고 있어 사전 승인의 필요성은 그다지 크다고 할 수 없다. 또한, 다른 한편으로는 클라우드 컴퓨팅 환경에서 국내 정보주체들의 개인정보 보호를 위하여 개인정보의 국외 이전을 금지해야 한다는 주장도 있을 수 있으나 글로벌 경제 환경에서 개인정보 국외이전을 금지하거나 지나치게 엄격하게 제한할 경우 자칫 우리나라만 고립될 수 있다.

개정안 신·구 대조표

현 행	개 정 안
<신 설>	제14조의2(국외 이전 개인정보의 보호 등) ① 개인정보처리자는 정보주체의 개인정보를 국외의 제3자에게 이전하려면 미리 다음 각 호의 모든 사항이 포함된 정보보호계약을 체결하여야 한다. 1. 제29조에 따른 개인정보보호를 위한 기술적·관리적 조치 2. 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 사항 3. 그 밖에 정보주체의 개인정보 보호를 위하여 필요한 조치 ② 보호위원회는 제1항 각 호의 모든 사항이 포함된 표준 정보보호계약서를 작성하여 개인정보처리자에게 사용을 권고할 수

	있다. ③ 보호위원회는 개인정보처리자 등의 요구가 있는 경우 개인정보를 이전받는 국가의 법령, 기술, 관행 등 전반적인 개인정보 보호 수준을 검토·평가(이하 이조에서 “수준평가”라 한다)하여 해당 국가를 개인정보 이전 적합 국가로 지정·고시할 수 있다. 이 경우 개인정보처리자는 제1항 및 제26조제7항에도 불구하고 개인정보를 이전받은 자가 해당 국가의 법령을 준수하는 것을 조건으로 개인정보를 국외로 이전할 수 있다. ④ 제3항에 따른 수준평가의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

3. 외국사례

미국, 일본 등 대부분의 나라에서 국외로 이전하는 개인정보에 대하여 법률에 별도의 보호 장치를 마련해 두고 있는 경우는 드물다. 그러나 유럽연합은 자국 국민의 개인정보를 보호하기 위하여 개인정보를 제3국이나 국제기구로 이전하고자 하는 경우에는 개인정보처리자나 프로세서(수탁자 등)가 2012년 EU Regulation에 따라 처리하는 것을 조건으로만 허용된다.[21] 이에 따라 개인정보를 국외로 이전하고자 하는 경우에는 원칙적으로 유럽연합 집행위원회 또는 개인정보보호기구의 사전 심사·승인을 받아야 한다. 국외 이전 심사·승인 방식은 크게 1) 개인정보 이전 적합 국가인지 여부를 판단해 지정·고시된 방법, 2) 표준 정보보호계약에 의한 방법, 3) 자체 정보보호계약에 의한 방법, 4) 구속력 있는 기업규칙(Binding Corporate Rules)에 의한 방법 등 네 가지로 나뉜다.

첫째, 유럽 집행위원회가 제3국이나 국제기구가 적절한 수준

21) 2012년 EU Regulation 제40조 참조. Article 40(General principle for transfers) Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization.

의 보호를 보증하고 있다고 판단하여 국외 이전 적합국가로 지정·고시한 경우에는 집행위원회의 추가적인 승인 절차를 거치지 않아도 개인정보 국외 이전이 가능하다. 집행위원회가 보호 수준의 적합성을 평가할 때에는 다음의 요소를 고려하여야 한다. (a) 개인정보보호 관련 법률의 존재 및 행정적·사법적 구제를 포함하여 효과적이고도 집행 가능한 정보주체의 권리, (b) 개인정보보호에 대하여 책임을 지는 하나 이상의 독립적인 개인정보보호기구의 존재, (c) 제3국 또는 국제기구가 체결한 국제협약.[22]이다.

---

22) 2012년 EU Regulation 제41조 참조. Article 41(Transfers with an adequacy decision) 1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organization in question ensures an adequate level of protection. Such transfer shall not require any further authorization.
2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements: (a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organization, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred; (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organization in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and (c) the international commitments the third country or international organization in question has entered into.

둘째, 유럽 집행위원회가 채택한 표준 정보보호계약 조항에 따라 개인정보처리자(또는 프로세서)와 개인정보 수령인 사이에 정보보호계약을 체결한 경우에는 유럽 집행위원회나 개인정보보호기구의 사전 승인 없이 국외 이전이 가능하다.[23]

셋째, 유럽 집행위원회가 채택한 표준 정보보호계약 조항에 따르지 않고 개인정보처리자(또는 프로세서)와 개인정보 수령인 사이에 법률적으로 구속력을 가진 임의의 정보보호계약을 체결한 경우에는 개인정보보호기구의 사전 승인을 받아야 한다.[24]

넷째, 특정 기업집단이 임직원을 포함하여 해당 기업집단내의 모든 구성원에게 적용되는 구속력이 있는 정보보호 사규(binding corporate rules)를 제정한 경우에는 개인정보보호기구의 사전 승인을 받아야 한다. 이 경우 해당 정보보호 사규는 정보주체에게 집행 가능한 권리를 명시적으로 부여하여야 하고, 최소한 다음 각 호의 모든 사항을 충족하고 있어야 한다. (a) 기업집단 및 그 구성원의 구조 및 상세 연락처, (b) 이전되는 개인정보의 범주, 개인정보의 처리 유형 및 목적, 영향을 받게 될 정보주체의 유형, 개인정보가 이전되는 제3국에 관한 정보, (c) 국내외를 막론한 법적 구속력, (d) 일반적인 정보보호 원칙(특히 목적 제한, 정보 품질, 처리의 법적 근거, 민감정

23) 2012년 EU Regulation 제42조제2항(b) 참조.
24) 2012년 EU Regulation 제42조제2항(d) 참조.

보의 처리, 정보보안 조치 등), (e) 정보주체의 권리 및 권리를 행사하기 위한 수단, (f) 제3국 기업에 의한 구속력 있는 기업 규칙의 침해에 대한 회원국 기업의 책임, (g) 구속력 있는 기업규칙의 내용을 정보주체에 제공하는 방법, (h) 구속력 있는 기업규칙의 준수 여부를 조사하고 기업집단 내에서의 교육 및 불만처리 등을 감독할 정보보호책임자의 역할, (i) 구속력 있는 기업규칙의 준수를 보증하기 위한 기업집단 내의 장치, (j) 변경 사항을 정책에 반영·기록하고 개인정보보호기구에 보고할 장치, (k) 기업집단 구성원의 준수를 보증하기 위한 개인정보보호기구와의 협력 메커니즘[25]이다.

---

25) 2012년 EU Regulation 제43조 참조. Article 43(Transfers by way of binding corporate rules) 1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they: (a) are legally binding and apply to and are enforced by every member within the controller''s or processor's group of undertakings, and include their employees; (b) expressly confer enforceable rights on data subjects; (c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules shall at least specify: (a) the structure and contact details of the group of undertakings and its members; (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question; (c) their legally binding nature, both internally and externally; (d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organizations which are not bound by the policies; (e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in

제2절 설계 및 설정 프라이버시 원칙의 도입 (제16조)

1. 현황 및 문제점

개인정보보호법은 개인정보 최소수집원칙을 채택하고 있으나 대다수 개인정보처리자들이 회원가입신청서, 개인정보활용동의서, 개인정보처리시스템 등을 개발할 때 이와 같은 원칙을 무시하고 있다. 오히려 가급적이면 많은 개인정보를 수집하여 오

---

accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules; (f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that member is not responsible for the event giving rise to the damage; (g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11; (h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling; (i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules; (j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority; (k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.

랜 동안 이용·제공할 수 있도록 동의서, 가입신청서 등의 양식을 만들고, 서비스를 구성할 때에도 고객 맞춤형 서비스를 제공한다는 명분으로 많은 개인정보를 수집·활용할 수 있도록 구성하며, 개인정보처리시스템도 구축할 때에도 최대한 많은 개인정보를 처리하도록 설계하고 있다.

개인정보처리에 대한 동의를 받을 때에도 동의를 유도하기 위하여 동의를 디폴트로 설정해 두거나 사실상 동의를 강요하는 형태의 동의방법을 사용한다. 공개 디폴트 설정은 특히 사회관계망서비스 등에서 광범위하게 활용되고 있으며, 은행 등에서도 계좌신청, 신용카드신청, 대출신청 등의 경우 동의란에 체크를 하여 사실상 동의를 하도록 유도하고 있다. 정보주체가 디폴트를 해제하거나 조정할 수 있게 하고 있다고 하더라도 정보주체는 그 기능을 모르는 경우가 많고 무심결에 또는 귀찮아서 디폴트가 설정된 상태로 가입하거나 이용하다가 뒤늦게 자신의 개인정보가 공개된 사실을 발견하고 놀라는 경우가 흔하다.

2. 개정방향

정보주체의 개인정보 자기통제권이 실질적으로 실현될 수 있도록 상품이나 서비스의 구상·기획 단계에서부터 개인정보를 최소한으로 수집하도록 설계하여야 하고(privacy by design),

개인정보처리에 대한 동의를 받음에 있어서도 동의를 강요하거나 유인하는 방법을 사용하지 못하도록 금지(privacy by default)하여야 한다. 정보주체에게 아무리 많은 권리를 부여해도 개인정보처리자가 기술적으로 이를 존중하지 아니하고 경시하거나 무시해 버리면 실효성 없는 권리가 되고 만다.

개정안 신·구 대조표

현 행	개 정 안
제16조(개인정보의 수집 제한) ① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다. ② 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는	제16조(개인정보의 수집 제한) ① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다. ② 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는

서비스의 제공을 거부하여서는 아니 된다. <신 설>	서비스의 제공을 거부하여서는 아니 된다. ③ 개인정보처리자는 상품 또는 서비스를 개발하거나 개인정보파일을 구축·변경하고자 한 때에는 필요한 최소한의 개인정보만 수집하도록 설계하여야 한다.
시행령 제17조(동의를 받는 방법) ① 개인정보처리자는 법 제22조에 따라 개인정보의 처리에 대하여 다음 각 호의 어느 하나에 해당하는 방법으로 정보주체의 동의를 받아야 한다. 1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법 2. 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하	시행령 제17조(동의를 받는 방법) ① 개인정보처리자는 법 제22조에 따라 개인정보의 처리에 대하여 다음 각 호의 어느 하나에 해당하는 방법으로 정보주체의 동의를 받아야 한다. 1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법 2. 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하

는 방법 3. 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법 4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법 5. 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받는 방법 6. 그 밖에 제1호부터 제5호까지의 규정에 따른 방법에 준하는 방법으로 동의 내용을 알리고 동의의 의사표시를 확인하는 방법 <신 설>	는 방법 3. 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법 4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법 5. 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받는 방법 6. 그 밖에 제1호부터 제5호까지의 규정에 따른 방법에 준하는 방법으로 동의 내용을 알리고 동의의 의사표시를 확인하는 방법 ② 개인정보처리자는 제1항에 따른 방법으로 정보

	주체의 동의를 받을 때 동의를 강요하거나 유도하는 방법 또는 표식을 사용하여서는 아니 된다.
② 개인정보처리자는 법 제22조제5항에 따라 만 제14세 미만 아동의 법정대리인의 동의를 받기 위하여 해당 아동으로부터 직접 법정대리인의 성명·연락처에 관한 정보를 수집할 수 있다.	③ 개인정보처리자는 법 제22조제5항에 따라 만 제14세 미만 아동의 법정대리인의 동의를 받기 위하여 해당 아동으로부터 직접 법정대리인의 성명·연락처에 관한 정보를 수집할 수 있다.
③ 중앙행정기관의 장은 제1항에 따른 동의방법 중 소관 분야의 개인정보처리자별 업무, 업종의 특성 및 정보주체의 수 등을 고려하여 적절한 동의방법에 관한 기준을 법 제12조제2항에 따른 개인정보 보호지침(이하 "개인정보 보호지침"이라 한다)으로 정하여 그 기준에 따라 동의를 받도록 개인정보처리자에게 권장할 수 있다.	④ 중앙행정기관의 장은 제1항에 따른 동의방법 중 소관 분야의 개인정보처리자별 업무, 업종의 특성 및 정보주체의 수 등을 고려하여 적절한 동의방법에 관한 기준을 법 제12조제2항에 따른 개인정보 보호지침(이하 "개인정보 보호지침"이라 한다)으로 정하여 그 기준에 따라 동의를 받도록 개인정보처리자에게 권장할 수 있다.

3. 외국사례

최근 유럽연합과 미국은 정보주체의 권리를 실질적으로 보호하기 위해서 이른바 설계 프라이버시(privacy by design) 원칙과 설정 프라이버시(privacy by default) 원칙을 채택하고 있다.

2012년 EU Regulation은 개인정보처리자는 개인정보의 처리 수단을 결정하거나 개인정보를 처리할 때 해당 처리가 법률에서 규정하고 있는 요구조건을 충족하고 정보주체의 권리를 보장하는 방법으로, 적절한 기술적·관리적 보호 조치와 절차를 이행해야 한다(privacy by design). 고 규정하고 있으며, 또한 개인정보처리자는 처리되는 개인정보의 양 및 보존기간과 관련하여 개인정보가 초기 설정 상태에서 특정한 처리 목적에 맞게 처리되고 이러한 목적의 범위를 넘어서 수집되거나 보관되지 않도록 조치해야 하며, 특히 이 같은 조치는 개인정보가 초기 설정 상태에서 많은 사람들이 접근 가능하도록 설정되지 않도록 해야 한다(privacy by default) 고 규정하고 있다.[26)]

26) Article 23(Data protection by design and by default) 1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary

한편, 2012년 3월에 공표된 미국 FTC의 소비자 프라이버시 보호를 위한 권고[27]에서도 개인정보처리자는 모든 조직을 통해서 또한 제품이나 서비스를 개발하는 모든 단계에 있어서 소비자의 프라이버시가 증진되도록 하여야 한다고 하여 적시하고 있다.

제3절 인터넷접속정보 등의 처리 제한 (제16조의2 신설)

1. 현황 및 문제점

개인정보 여부를 판단함에 있어서는 특정 개인의 식별성이

---

for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.

4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

27) FTC, Protecting Consumer Privacy in an Era of Rapid Change, RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, FTC REPORT, MARCH 2012, PP.22-34 참조.

매우 중요한 개념이다. 그러나 식별성은 상대적인 개념이어서 하나의 데이터가 어떤 경우에는 개인정보가 될 수 있는가 하면 다른 경우에는 개인정보로 볼 수 없는 경우가 있다. 개인정보의 정의상 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 개인정보로 보기 때문에[28] 같은 데이터라 하더라도 다른 정보와 쉽게 결합해서 특정 개인을 알아볼 수 있으면 개인정보이고 다른 정보와 쉽게 결합할 수 있는 상황이 아니어서 특정 개인을 알아 볼 수 없다면 개인정보가 아니다.

특히 빅데이터 환경에서 가장 관심을 끌고 있는 인터넷접속정보, 인터넷프로토콜 주소, 로그기록, 사물의 위치정보, 각종 비정형정보 등이 개인정보에 해당하는지 여부를 판단하기 위해서는 다른 정보와 쉽게 결합할 수 있는지 여부를 판단해야 한다. 따라서 이들 정보를 수집·이용하고자 하는 개인정보처리자는 해당 정보들이 다른 정보와 쉽게 결합할 수 있는 조건에 있는지 여부를 항상 주의 깊게 살펴야 한다. 그런데 어떤 정보가 다른 정보와 쉽게 결합하여 특정인을 식별할 수 있는 조건에 있는지 여부를 판단하는 것은 상당히 주관적일 수 있다. 때문에 실무에서는 이들 정보가 이름, 연락처 등과 결합되

28) 개인정보보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. 1. “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

어 있지 아니하면 개인정보로 보지 않으려는 경향이 강하고, 이들 정보를 수집·분석해서 맞춤형 광고 등에 활용하는 사례가 늘고 있다.

2. 개정방향

인터넷접속정보, 인터넷프로토콜 주소, 로그기록, 사물의 위치정보 등은 익명으로 수집·이용되고 있다고 하더라도 다른 정보와 쉽게 결합하여 정보주체를 식별할 수 있는 경우가 많고 정보의 활용 가치도 매우 크다. 따라서 이들 정보는 case by case로 개인정보에 해당하는지 여부를 판단하는 것보다는 처음부터 아예 개인정보로 간주해 버리는 것이 정보주체의 이익 보호에 부합하고 법집행 상의 혼란도 피할 수 있다. 즉 이들 정보가 개인정보에 해당하는지 여부를 일일이 따지지 않고 법률적으로 항상 개인정보로 보아 버리는 것이다.

이들 정보를 개인정보로 보게 되면, 개인정보처리자는 정보주체가 요구하거나 신청한 서비스의 제공을 위하여 불가피하게 필요한 경우에만 그 범위 내에서 정보주체의 동의 없이 해당 정보를 수집·이용하거나 제공할 수 있다. 그러나 정보주체가 해당 서비스의 이용을 중단한 경우에는 즉시 이들 정보의 수집·생성을 중단하거나 정보주체가 정보의 수집·생성을 언제든지 차단할 수 있도록 인터넷 추적 차단기능(Do-Not-Track)

을 제공하도록 하여야 한다.

일부에서는 오히려 이와 같은 정보까지 개인정보로 보게 되면 개인정보의 범위가 무한정 확대되어 개인정보의 활용에 현저한 지장이 따른 다거나 빅데이터가 불가능해진다고 비판한다. 따라서 개인정보의 정의 중 “해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다.”라는 부분을 삭제해야 한다거나 익명정보에 대해서는 보호수준을 차등화해서 이들 정보는 정보주체의 동의 없이도 자유롭게 수집·이용할 수 있도록 하여야 한다고 주장하기도 한다. 그러나 단지 이름과 분리된 정보라고 해서 그것만으로 개인정보보호법의 보호대상에서 제외시키는 것은 정보주체의 권리를 현저히 침해할 우려가 있고, 사실상 국제적으로 확립된 개인정보에 관한 정의를 변경한다는 것은 글로벌 경제 환경에서 맞지 않다. 또한 개인에 대한 추적으로부터 개인의 사생활 보호를 강화하려는 국제적은 흐름에 역행한다. 예컨대 맞춤형 광고에 이용되는 정보들은 주로 익명정보로 존재하는 경우가 많지만, 개인에 대한 추적이 사생활 침해 위험이 크기 때문에 Do-not-Track제도를 도입한 것이다.

개정안 신·구 대조표

현 행	개 정 안

<신 설>	제16조의2(인터넷접속정보 등의 수집·이용 등) ① 개인정보처리자는 정보주체가 요구하거나 신청한 정보통신서비스의 제공을 위하여 자동적으로 생성되거나 수집된 정보(인터넷접속정보, 인터넷프로토콜 주소, 로그기록, 통신단말기 위치정보 등)를 그 서비스의 제공 또는 이행에 필요한 범위 내에서 정보주체의 동의 없이 수집·이용하거나 제공할 수 있다. ② 개인정보처리자는 정보주체가 해당 정보통신서비스의 이용을 중단한 경우에는 제1항에 따른 정보의 수집·생성을 즉시 중단하거나 정보주체가 정보의 수집·생성을 언제든지 차단할 수 있는 기능을 제공하여야 한다. ③ 개인정보처리자는 제1항에 따라 수집 또는 생성된 정보를 해당 정보통신서비스의 제공 또는 이행

	을 위한 목적 외로 이용 또는 제공하고자 하는 경우에는 미리 정보주체에게 제18조제3항 각 호의 모든 사항을 알리고 동의를 받아야 한다.

3. 외국사례

미국, 일본 등은 인터넷접속정보, 인터넷프로토콜 주소, 로그기록, 사물의 위치정보 등이 개인정보에 해당하는지 여부를 여전히 개인정보의 해석에 맡기고 있다. 다시 말해 다른 정보와 쉽게 결합해서 특정 개인을 식별할 수 있는 조건에 있는지 여부에 따라 개별적으로 판단하고 있다. 이에 반하여 유럽연합은 이를 입법적으로 해결하고 있다. 2009년 개정 EU ePrivacy Directive[29]는 이른바 '쿠키(cookie) 정보'의 수집·이용을 제한하는 규정을 두고 있다. EU는 2009년 11월 25일에 2002년 제정된 ePrivacy Directive을 대폭 개정하였는데, 개정 법률의 핵심 내용 중 하나는 통신 단말기에 어떤 정보를 저장하는 행위

29) 정식 명칭은 「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 sector (Directive on privacy and electronic communications)」이다.

나 저장되어 있는 정보를 수집하는 행위를 제한하는 것이다. 단말기에 저장하거나 저장된 정보란 주로 “쿠키”를 말하지만, 기술 중립적으로 표현하기 위하여 쿠키라는 단어를 사용하고 있지는 않다. 이에 따라 EU에서는 쿠키를 개인정보로 보든 보지 않던 마케팅 등의 목적으로 쿠키정보를 저장하거나 수집하는 행위에 대하여는 정보주체의 동의가 필요하다.

따라서, 개인정보처리자가 전자통신서비스 이용자 또는 가입자의 단말기에 정보를 저장하거나 저장되어 있는 정보를 수집하고자 할 때에는 사전에 해당 이용자 또는 가입자의 동의를 받아야 한다(OPT-IN). 이와 같은 동의는 1995년 EU 개인정보보호지침에 따라, 특히 그 중에서도 정보의 처리목적에 대하여 명확하고도 종합적인 정보(clear and comprehensive information)를 제공하고 받은 동의이어야 한다(제5조(3) 전단). 다만, 전자통신네트워크를 통한 통신의 전달을 수행할 목적으로만 또는 서비스 가입자 또는 이용자가 명시적으로 요구한 정보사회서비스(an information society service)의 제공을 위하여 반드시 필요한 경우 기술적인 저장이나 접근행위(technical storage or access)에 대하여는 고지 및 동의가 필요하지 않다(제5조(3) 후단).[30]

30) Article 5 (3) Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about

제4절 개인정보 결합·통합·연동 기준 등 신설 (제18조의2 신설)

1. 현황 및 문제점

ICT 환경이 빅데이터 환경에 접어들면서 기업들이 보다 정확한 맞춤형 광고 및 서비스를 위해 데이터의의 결합, 조합, 연동, 통합 등에 사활을 걸고 있다. 이와 같은 데이터의 결합, 조합, 통합, 연동 등은 궁극적으로 개인의 성격, 성향, 취미, 건강, 선호, 평판, 경제력, 위치 등을 분석·평가할 목적으로 이루어지고 있어 사생활 침해 위험이 매우 크다. 빅데이터가 빅브라더로 악용될 수 있는 이유이다. 이미 구글, 네이버 등을 포함한 많은 기업들이 개인정보의 단순한 조합이나 결합의 수준을 벗어나서, 더 나아가서는 서비스별 개인정보의 집합 관리·저장 수준을 벗어나서 각각의 다른 서비스에 이용되고 있는 개인정보 DB를 모두 하나로 통합하거나 연동하는 수준으로까지 확대되고 있다.

---

the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

개인정보보호법은 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보 등 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보를 민감정보라고 하여 원칙적으로 수집·처리를 금지하고 있고 필요한 경우에는 정보주체의 별도 동의를 얻어서 이용하라고 되어 있지만,[31] 이와 같은 민감정보들만이 아니라 그 밖의 파편적인 조각 정보들도 이들을 모아 결합하고 조합하고 통합하면 민감정보보다 더 사생활 침해 위험이 큰 민감정보가 될 수 있다. 하지만 개인정보보호법은 이와 같은 파편적 또는 단편적인 조각 정보들의 결합, 가공, 조합, 통합, 연동 등에 대해서는 명확한 기준이 없다.

2. 개정방향

이미 정보주체의 동의를 받거나 다른 사유로 적법하게 수집·이용하고 있는 개인정보들도 이들 정보를 다시 결합, 가공, 조합, 통합, 연동 등을 하면 위험성이 확대되고 개인정보의 최소처리원칙에도 어긋난다. 따라서 개인정보처리자가 개인의 성격, 성향, 취미, 건강, 선호, 평판, 경제력, 위치 등을 분석·평가할 목적으로 적법하게 수집·생성된 정보들을 전자적인

31) 개인정보보호법 제23조 참조.

방법으로 결합, 조합, 통합, 연동 등(이하 '결합 등'이라 한다)을 하고자 하는 경우에는 정보주체에게 분석·평가의 목적, 결합 등의 대상이 되는 개인정보의 항목·유형 등을 알리고 동의를 받도록 하여야 한다. 또한 정보주체는 개인정보의 분석·평가 또는 결합 등을 언제든지 거부할 권리를 가져야 하며 이 경우 특별한 사유가 없는 한 개인정보처리자는 분석·평가 또는 결합 등을 즉시 중단하여야 한다.

다만, 법률의 규정, 계약의 체결 및 이행 등을 위하여 필요한 경우와 같이 개인정보의 결합 등이 불가피하게 필요할 경우가 있을 수 있으므로 개인정보보호법 제15조제1항 각 호의 사유가 있는 경우나 정보 정확성의 원칙에 따라 수집·보관 중인 개인정보를 단순히 갱신하기 위하여 필요한 경우 예컨대 바뀐 옛날 주소나 전화번호의 수정 등의 경우에는 정보주체의 동의를 받지 않고도 결합 등이 가능하도록 하여야 할 것이다. 이와 같은 동의의 예외는 정보주체의 동의를 받았거나 그 밖의 사유로 이미 적법하게 수집·이용되고 있는 개인정보에 한하여야 한다.

개정안 신·구 대조표

현 행	개 정 안
<신 설>	제18조의2(분석·평가 목적

	의 정보 결합 등) ① 개인정보처리자는 개인의 성격, 성향, 취미, 건강, 선호, 평판, 경제력, 위치 등을 분석·평가할 목적으로 적법하게 수집·생성된 정보들을 전자적인 방법으로 결합, 조합, 통합, 연동 등(이하 “결합 등”이라 한다)을 하고자 하는 경우에는 다음 각 호의 모든 사항을 정보주체에게 알리고 동의를 받아야 한다. 1. 분석·평가의 목적 2. 결합 등의 대상이 되는 정보의 항목 또는 정보의 구체적인 유형 ② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 동의 없이 정보의 결합 등을 할 수 있다. 1. 법률에 특별한 규정이 있거나 법령상 의무를 준

	수하기 위하여 불가피한 경우 2. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우 3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 4. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다. ③ 정보주체는 제1항에 따

	른 분석·평가 또는 정보의 결합 등을 언제든지 거부할 권리를 가진다. 이 경우 제2항 각 호에 해당하는 사유가 없으면 개인정보처리자는 분석·평가 또는 결합 등을 즉시 중단하여야 한다.

3. 외국사례

유럽연합에서는 개인정보의 처리에 관한 일반원칙이 개인정보의 수집·이용, 제공, 목적 외 이용·제공 등의 경우뿐만 아니라 개인정보의 결합 등의 경우에도 그대로 적용되기 때문에 원칙적으로 정보주체의 명시적인 동의가 있거나 그 밖의 정당한 사유가 존재하지 아니하는 한 개인정보의 결합 등은 허용되지 않는다고 보아야 한다. 2012년 EU Regulation은 「개인

정보의 처리(processing)란 자동화된 수단에 의하는지의 여부와 관계없이 수집, 기록, 조직, 구성, 보관, 수정 또는 변경, 복구, 참조, 사용, 전송에 의한 공개, 유포 또는 살포, 결합 또는 배합, 삭제 또는 파괴 등과 같이 개인정보 또는 일련의 개인정보에 대해서 수행하는 공정 또는 일련의 공정들을 의미한다.」라고 규정하고 있고,[32] Regulation 제6조는 개인정보 "처리"는 다음 중 하나 이상이 적용되는 경우에만 적법하다고 규정하고 있기 때문이다.

(a) 정보주체가 하나 이상의 구체적인 목적을 위해 자신의 개인정보 처리에 대하여 동의를 한 경우

(b) 정보주체가 계약 당사자인 계약의 이행을 위해 또는 계약 체결 전 정보주체의 요청에 따라 조치를 취하기 위하여 개인정보 처리가 필요한 경우

(c) 개인정보처리자가 의무의 주체인 법률상의 의무를 준수하는데 필요한 경우

32) 2012년 EU Regulation 제4조제3항 참조. (3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;

(d) 정보주체의 중요한 이익을 보호하기 위하여 필요한 경우

(e) 공공의 이익을 위해 필요하거나 또는 개인정보처리자에게 부여된 공적인 권한의 행사를 위해 필요한 경우

(f) 개인정보처리자가 추구하는 적법한 이익의 목적에 부합하는 경우(다만, 정보주체 특히 정보주체가 어린이인 경우 정보주체의 이익 또는 기본적 권리 및 자유가 우선될 때는 제외)

(g) 제83조에서 정한 규정 및 보호수단에 따라 역사, 통계, 과학 연구 목적으로 필요한 경우

이와 같이 유럽연합에서는 개인정보의 처리원칙이 우리나라와 달리 개인정보의 수집·이용, 제공, 목적 외 이용·제공, 처리위탁 등의 경우에만 제한적으로 적용되는 것이 아니라 결합 등을 포함한 개인정보처리 일반에 적용된다.

한편, 2012년 EU Regulation은 「모든 자연인은 자신에 관한 사적인 측면(personal aspects)을 평가하거나 특히 자신의 업무능력, 경제적 상황, 위치정보, 건강상태, 개인적 선호, 신뢰성, 행태 등을 분석하거나 예측하기 위한 의도로써 오로지 자동화된 처리방법에 의존하고 있고 자신과 관련된 법률적 효과를 발생시키거나 자신에게 중대한 영향을 미치는 경우 해당

처리의 대상이 되지 아니할 권리를 가진다.」라고 하여 프로파일링에 대한 거부권을 명시적으로 규정하고 있다. 다만, 다음과 같은 경우에는 자동화된 프로파일링이 허용된다.[33]

(a) 정보주체가 청약을 한 계약의 체결이나 이행을 위하여 필요한 경우로써 정보주체의 요청이 있거나 정보주체의 적법한 이익을 보호해 주는 적절한 조치가 마련되어 있는 경우(예컨대 해당 평가나 판단에 사람이 참여할 권리가 보장된 경우)로써 계약을 체결되거나 이행하는 과정에서 수행되는 경우

(b) 정보주체의 정당한 이익을 보호하기 위한 적절한 조치

---

33) 2012년 EU Regulation 제20조 참조. 제20조에서 규정하고 있는 "프로파일링에 근거한 측정"은 1995년 EU Directive 제15조(개인에 대한 자동화된 결정)에서 유래한 것이다. Article 15(Automated individual decisions) 1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.
2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:
(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

들을 규정하고 있는 유럽연합 또는 회원국의 법률에 의해 명시적으로 수권을 받은 경우

(c) 제7조(고지의무)에서 규정한 조건과 적절한 안전장치에 따라 그리고 정보주체의 동의를 받고 처리되는 경우

제5절 영리목적의 개인정보 판매·대여 등 제한(제18조의3 신설)

1. 현황 및 문제점

우리나라에서 개인정보가 가장 심각하게 문제되고 있는 것 중 하나는 개인정보의 양도, 대여 등이다. 현행법상 개인정보의 양도, 대여 등은 개인정보의 목적 외 제공에 해당하여 정보주체의 별도 동의를 받아야 한다.[34] 그러나 실무적으로는 대부분 개인정보를 수집할 때 미리 제3자 제공에 대해서 동의를 받아 두고 있는 것이 일반적인 추세이다. 이와 같이 온·오프라인을 불문하고 정보주체의 동의를 받았다는 명분과 근거만으로 개인정보가 광범위하게 거래되고 있다.

34) 개인정보보호법 제18조제2항 제1호 참조.

기업 간에 개인정보를 서로 팔고사면서 개인정보가 광범위하게 목적 외로 이용되고 있을 뿐만 아니라 사고 판 개인정보를 결합 등을 하여 새로운 정보를 생산해 내는 등 사생활 침해 위험이 크지만 정작 정보주체는 자신의 개인정보가 여러 사업자들 간에 거래되고 있다는 사실을 모르는 경우가 많다.

대부분의 정보주체들이 서비스 가입단계나 물품 구입단계에서 개인정보 제3자 제공에 대해서 무심코 동의를 하고 있지만, 자신의 개인정보가 영리목적으로 전전유통 될 수 있다는 사실을 모른 상태에서 동의하기 때문이다. 따라서 '영리 목적으로' 개인정보를 사고팔거나 대여하는 행위에 대하여는 정보주체의 동의를 받을 때 그 목적을 보다 명확하게 할 필요가 있다.

2. 개정방향

개인정보처리자가 대가를 목적으로 다른 사람에게 개인정보의 제공 등에 대한 동의를 받고자 하는 경우에는 다른 개인정보처리에 대한 동의와 구분하여 '별도의 동의'를 받도록 하여야 한다. 개인정보 제3자 제공에 대해서는 원칙적으로 정보주체의 동의를 받도록 되어 있으나, 개정안은 영리 목적의 개인정보 판매, 대여 등에 대해서는 특별히 '별도의 동의'를 받으라는 것이 특징이라고 할 수 있다.

우리나라는 아주 특수한 경우를 제외하고는 대부분의 개인정보처리에 대해서 정보주체의 동의를 받도록 요구하고 있어 동의가 남용되고 있다. 즉 거래를 위해서 기본적으로 요구되는 개인정보에 대해서도 동의를 받도록 요구하는 경우가 많아 오남용 가능성이 희박한 개인정보의 처리에 대한 동의와 사생활 침해 위험이 큰 개인정보의 판매, 대여 등에 대한 동의가 혼재되어 있어 정보주체가 이를 인식하기 어렵다. 따라서 영리를 목적으로 개인정보를 판매, 대여 등을 하는 경우와 그 밖의 목적으로 개인정보를 제공하는 경우를 구분하여 전자에 대해서는 별도의 동의를 받도록 하는 것이 우리나라 현실에 부합한다고 할 수 있다.

또한, 판매, 대여 등에 대한 동의를 받은 시기와 실제 개인정보를 제공 또는 이전하는 시기가 다른 경우에는 제공 또는 이전을 할 때마다 대통령령으로 정하는 방법으로 정보주체에게 제공 또는 이전의 사실과 함께 판매, 대여 등에 대한 동의를 받은 날짜와 근거를 알리도록 하여야 한다. 다만, 정보주체가 판매, 대여 등의 사실에 대한 통지를 받기를 거부한 경우에는 제외하도록 한다. 개인정보의 제공 또는 이전이 반복적으로 행해지고 있는 경우 통지 자체가 또 다른 사생활 침해를 유발할 수 있기 때문이다.

개정안 신·구 대조표

현 행	개 정 안
<신 설>	제18조의3(영리목적의 개인정보 제공 등) ① 개인정보처리자는 매매, 대여 등 대가를 목적으로 한 개인정보의 공개 등에 대한 동의를 받고자 하는 경우에는 정보주체가 이를 명확하게 인지할 수 있도록 제17조제2항, 제18조제3항 각 호의 사항을 별도로 알리고 동의를 받아야 한다. ② 제1항에 따라 개인정보의 공개 등에 대한 동의를 받은 시기와 실제 공개 등을 하는 시기가 다른 경우에는 공개 등을 할 때마다 대통령령으로 정하는 방법으로 정보주체에게 제17조제2항 또는 제18조제3항 각 호의 모든 사항과 함께 그 출처(동의의 근거와 날짜)를 알려야 한다. 다만,

	정보주체가 통지를 받기를 거부한 경우에는 그러하지 아니한다.

3. 외국사례

유럽연합 개인정보보호법안은 정보주체가 특정한 목적으로 자신의 개인정보가 처리된다는 것에 동의했다는 사실을 입증해야 할 책임을 개인정보처리자가 부담하도록 하는 것 외에, 개인정보처리에 대한 정보주체의 동의가 다른 문제와 관련된 서면 진술에 포함되는 경우에는 다른 문제와 구별될 수 있도록 해서 동의의 요건을 제시하도록 요구하고 있다.[35] 뿐만 아니라 개인정보가 다이렉트 마케팅(direct marketing)을 위해

35) 2012년 EU Regulation 제7조 참조. Article 7(Conditions for consent)
1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.
2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.

처리되는 경우에는 정보주체가 아무런 비용 부담 없이 자신의 개인정보가 이러한 마케팅을 위해 처리되는 것에 반대할 수 있는 권리를 가져야 하며, 이러한 정보주체의 권리는 명확한 방식으로 정보주체에게 분명하게 제시되어야 하고 다른 정보와 뚜렷하게 구별되어야 있어야 한다.[36] 이처럼 2012년 EU Regulation은 개인정보의 매매, 대여 등 대가를 목적으로 하는 개인정보의 공개 등에 한정하지 아니하고 다이렉트 마케팅을 위해 처리되는 개인정보 일반에 대하여 별도의 고지를 하도록 요구하고 있다. 그러나 다이렉트 마케팅을 위한 개인정보처리에 대해서까지 별도로 고지하고 동의를 받도록 할 경우 제3자에게 개인정보의 이전이나 제공이 없는 경우에도 별도의 고지·동의를 해야 하기 때문에 고지·동의 절차가 형식화할 우려가 있다.

---

36) 2012년 EU Regulation 제19조 참조. Article 19(Right to object) 1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.
3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.

제6절 정보주체 이외로부터 수집한 개인정보의 통지의무 강화 (제20조)

1. 현황 및 문제점

개인정보처리자가 개인정보를 정보주체로부터 직접 수집하지 아니하고 제3자(거래처, 관공서, 공개정보 등)로부터 수집·보관·이용·제공하는 경우 정보주체는 그 사실을 알기 어렵다. 또한 정보주체가 개인정보 제3자 제공에 동의한 경우 제공받는 자는 정보주체에게 별도의 고지 또는 동의 절차 없이 개인정보를 수집·이용할 수 있지만, 현행 개인정보보호법은 정보주체 이외로부터 개인정보를 수집한 경우 정보주체의 요구가 있는 때에만 수집출처, 처리목적 등을 고지해 주면 된다. 따라서 정보주체가 개인정보 제3자 제공에 대하여 동의한 사실과 이 동의에 기해서 제3자가 개인정보처리자로부터 수집해서 실제로 이용하는 개인정보처리 사이의 관계를 알기 어렵다.

정보주체는 다양한 거래 또는 다양한 관계에서 제3자 제공에 대해서 동의를 해야 하는 경우가 많고, 자신이 제3자 제공에 대해서 동의한 사실을 모두 기억하기 어려우며, 제3자 제공에 대하여 부주의하게 동의한 경우도 적지 아니하나, 현행법 하에서는 정보주체의 요구가 없으면 고지할 의무가 없어 정보주체가 처리정지 요구권 행사에 어려움이 따를 수밖에 없는 상태

이다. 특히 최근 빅데이터 기술의 발달에 따라 정보주체 이외로부터 수집한 개인정보의 수와 종류가 급속히 확대될 전망이어서 개인정보처리자가 자신이 정보주체 이외로부터 수집해서 보관하고 있는 개인정보를 정보주체에게 스스로 알려주지 아니하면 정보주체는 개인정보처리자가 자신에 관하여 어떠한 개인정보를, 어떤 경로를 통해서, 어떻게 수집·보관·이용하고 있는지를 알기 어렵다.

2. 개정방향

개인정보처리자는 정보주체의 요구가 있는 경우뿐만 아니라 정보주체의 요구가 없더라도 정보주체 이외로부터 수집한 개인정보를 이용 또는 제공하고자 하는 때에는 정보주체에 대하여 통지의무를 부과하도록 한다. 정보주체가 개인정보 자기통제권을 충분히 행사할 수 있도록 보장하기 위한 것이다. 통지의무의 내용도 개인정보를 수집한 출처와 근거, 수집한 개인정보의 항목, 개인정보의 처리 목적, 처리정지 요구권 등으로 확대해야 한다.

정보주체 이외로부터의 개인정보 수집은 대부분 적법하게 사용이 허락된 공개된 개인정보이거나, 법령에 따라 수집·이용이 허락된 개인정보이거나, 정보주체가 제3자 제공에 동의한 개인정보이므로 정보주체 이외로부터 수집한 개인정보의 수집

출처 등 고지의무는 불필요하다는 주장이 있을 수 있고, 개인정보처리자에게 과도한 비용을 유발한다는 주장이 있을 수 있다. 그러나 공개된 개인정보라도 적법하게 이용되지 않거나, 법령상 수집·이용이 허가된 개인정보 또는 정보주체가 제3자 제공에 동의한 개인정보라도 그 취지에 맞지 않게 이용·제공되는 경우가 있을 수 있으므로 정보주체는 자신이 직접 제공하지 아니한 개인정보의 처리 내역을 확인할 기회와 권리를 가져야 한다.

혹자는 개인정보보호법 제20조가 불법으로 수집한 개인정보에 대해서 추후에 개인정보처리자가 정보주체에게 수집출처, 처리목적, 정보주체의 권리 등을 알려주면 사후 추인을 규정한 것으로 오해하고 있으나, 반대로 제20조는 불법으로 수집·처리되고 있는 개인정보를 색출하여 정보주체가 개인정보 자기통제권을 행사할 수 있도록 기회를 주고자 도입된 것이다.

개정안 신·구 대조표

현 행	개 정 안
제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를	제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를

처리하는 때에는 정보주체의 요구가 있으면 즉시 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.	처리하는 경우에는 해당 개인정보를 최초로 이용 또는 제공할 때까지 다음 각 호의 모든 사항을 정보주체에게 알려야 한다. 정보주체의 요구가 있는 때에도 같다.
1. 개인정보의 수집 출처	1. 개인정보의 수집 출처 및 근거
<신 설>	2. 수집한 개인정보의 항목
2. 개인정보의 처리 목적	3. 개인정보의 처리 목적
3. 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실	4. 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실
② 제1항은 다음 각 호의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다.	② 제1항은 다음 각 호의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다.
1. 고지를 요구하는 대상이 되는 개인정보가 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우	1. 고지를 요구하는 대상이 되는 개인정보가 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우
2. 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의	2. 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의

재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우	재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

3. 외국사례

2012년 EU Regulation은 개인정보가 정보주체로부터 직접 수집되지 않는 경우 개인정보처리자는 다음 각 호의 모든 사항과 함께, 해당 개인정보를 어디에서 수집하였는지를 정보주체에게 알려야 한다. 이와 같은 통지의무의 이행 시기는 정보주체 이외로부터 수집한 개인정보를 기록할 때 또는 개인정보가 수집되거나 처리되는 특정한 상황을 고려하여 수집된 후 합리적인 일정 기간 후 또는 다른 수령인에게 정보가 공개될 것이라고 예상되는 경우에는 적어도 정보가 처음 공개될 때까지 통지하여야 한다.[37]

(a) 개인정보처리자(가능한 경우 개인정보처리자의 대리인 및 정보보호 담당자 포함)의 신원 및 연락처

(b) 개인정보가 제6조 (1)항 (b)에 의하여 처리되는 경우

37) 2012년 EU Regulation 제14조 참조.

계약 조건 및 일반 조건, 그리고 개인정보가제6조 (1)항 (f)에 의하여 처리되는 경우에는 개인정보처리자가 추구하는 적법한 이익을 포함하여 개인정보가 처리되는 목적

(c) 개인정보가 보관되는 기간

(d) 개인정보의 접근 및 수정 또는 삭제를 요구하거나 이러한 개인정보의 처리를 반대할 수 있는 권리의 존재 여부

(e) 감독기관에게 불만 사항을 제기할 수 있는 권리와 감독기관에 대한 상세 연락처 정보

(f) 개인정보 수령인 또는 수령인의 범주

(g) 유럽 집행위원회의 적절한 결정에 따라 제3국이나 국제기구가 제공하는 보호조치 하에서 개인정보처리자가 제3국이나 국제기구에게 개인정보를 이전하려고 하는 목적

(h) 개인정보가 수집되는 특정한 상황 하에서 정보주체와 관련된 개인정보의 공정한 처리를 보증하기 위해 필요한 추가적인 정보

다만, 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보처리자는 수집출처 등의 통지의무가 없다.

(a) 정보주체가 이미 통지내용에 대해서 알고 있는 경우

(b) 통지내용을 알리는 것이 불가능하거나 불필요한 경우

(c) 법률에 개인정보의 기록이나 공개가 규정되어 있는 경우

(d) 통지내용의 제공이 제21조에 따른 유럽연합 또는 회원국 법률에서 규정한 다른 사람의 권리나 자유를 침해하는 경우

제7절 민감정보의 처리 제한 (제23조)

1. 현황 및 문제점

민감정보는 정부・고용주・교육기관 등에 의하여 차별적으로 이용될 위험이 크기 때문에 우리나라 개인정보보호법은 민감정보의 처리를 원칙적으로 금지하고 있다. 그러나 개인정보보호법은 정보주체의 별도 동의가 있으면 언제든지 민감정보를

수집·이용·제공할 수 있게 되어 있어 민감정보 보호의 실효성이 떨어진다. 특히 사용자가 근로자를 채용할 때 또는 고용주가 근로자를 감시·관리할 목적으로 민감정보의 제출을 요구할 경우 근로자는 사실상 이를 거부하기 어렵다.

한편 현행 개인정보보호법은 민감정보를 처리할 수 있는 경우를 정보주체의 별도의 동의가 있거나 법령에서 민감정보의 처리를 요구하거나 허용하는 경우로 제한하고 있어 근로계약의 체결 및 이행, 진료의 진단 및 개시, 의학의 연구 및 방역, 소송의 제기 및 방어 등을 위해서 불가피하게 필요한 경우에도 정보주체의 별도의 동의가 있어야만 민감정보를 수집·처리할 수 있도록 규정하고 있어 정상적인 경제·사회 활동이 어렵게 하고 있다.

2. 개정방향

노동관계나 진료현장에서 민감정보가 필요 이상으로 수집·처리되지 않도록 하기 위해서는 정보주체의 동의가 있더라도 민감정보의 수집·처리는 원칙적으로 금지하고 예외적으로만 허용하여야 한다. 반면, 법률에 별도의 규정이 있거나 소송목적, 진료목적, 고용목적 등과 같이 민감정보의 처리가 불가피한 경우에는 제한적으로 처리를 허용하여 민감정보 처리에 따르는 시비를 제거하여야 할 것이다. 예컨대 사용자는 노동관계

법상 자신에게 부여된 의무이행이나 권리행사를 위해 불가피하게 필요한 경우에는 건강에 관한 정보를 수집하여 이용할 수 있게 하여야 한다.

정보주체의 명시적인 동의에 의해서도 민감정보의 처리를 금지하는 것은 헌법재판소가 인정한 개인정보자기결정권이나 사적 자치의 원칙에 어긋날 수 있다는 비판이 있을 수 있으나, 개인정보에 대한 정보주체의 권리는 인격권적인 성격이 포함되어 있고 개인정보자기결정권이라는 것도 정보주체의 권리를 보호하기 위한 것이므로 정보주체에 대한 차별적인 결과를 낳을 가능성이 큰 민감정보의 처리를 금지하는 것은 개인정보자기결정권의 목적 또는 취지에 반하는 것이라고 할 수 없다. 또한 국제결혼중개 등과 같이 업무의 성격상 민감정보의 수집이 불가피하게 필요한 경우에는 해당 법률에서 제한적으로 허용하는 것이 바람직하다.

개정안 신·구 대조표

현 행	개 정 안
제23조(민감정보의 처리 제한) 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의	제23조(민감정보의 처리 제한) ① 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주

사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 “민감정보“라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. 1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우 2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우	체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 “민감정보“라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. 1. 법률에서 구체적으로 해당 민감정보의 처리를 요구하거나 허용하는 경우 2. 공공기관이 법률에서 정하는 소관 업무수행을 위해 해당 민감정보의 처리가 불가피하게 필요한 경우 3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필

	요하다고 인정되는 경우 4. 소송의 제기·수행·방어를 위해 해당 민감정보의 처리가 필요한 경우 5. 진료·보건·예방의학·건강관리 등을 목적으로 해당 분야의 자격을 가진 자에 의하여 필요한 경우(관련 법령에 따라 비밀보호의무를 지는 자에 한한다) 6. 노동관계법상 사용자의 의무이행 및 권리행사를 위해 불가피하게 필요한 경우(건강정보에 한한다)
<신 설>	② 개인정보처리자는 제1항 각 호의 하나에 해당하여 민감정보를 처리할 때에는 필요한 최소한의 정보를 최소한의 기간만 처리하여야 한다. 이 경우 최소한의 정보 또는 기간이라는 입증책임은 개인정보처리자가 진다.

3. 외국사례

1980년 OECD 개인정보보호 가이드라인과 일본 개인정보보호법은 민감정보에 대한 개념이 없다. 그러나 2012년 EU Regulation을 '특별한 범주의 개인정보'라고 하여 민감정보의 개념을 도입하고 있으며 다른 개인정보와 구분해서 별도의 보호 장치를 마련해 두고 있다.[38] EU법상 '특별한 범주의 개인정보'에 해당하는 것으로는 인종, 출신 민족, 정치적 견해, 종교 및 신념, 노동조합 가입 여부, 유전자 정보, 건강정보, 성생활, 형사 판결 또는 보안 처분 등에 관한 정보이며 이와 같은 개인정보는 원칙적으로 처리가 금지된다.

다만, 다음 각 호의 어느 하나에 해당하는 경우에는 특별한 범주에 속하는 개인정보를 처리할 수 있다. 아래 (a)에서 보는 바와 같이 2012년 EU Regulation은 정보주체의 명시적인 동의가 있으면 특별한 범주의 개인정보를 처리할 수 있는 것으로 되어 있지만, 동조 단서는 유럽연합이나 회원국의 법률이 특별한 범주의 개인정보의 처리 금지 규정을 정보주체의 동의에 의해서 포기·취소할 수 없게 규정한 경우에는 정보주체의 동의에 의한 특별한 범주의 개인정보 처리를 금지하고 있다.

(a) 정보주체가 제7조(명시적 고지에 따른 동의) 및 제8조

38) 2012년 EU Regulation 제9조 참조.

(아동의 개인정보처리)에서 규정된 조건에 따라 개인정보를 처리하는 것에 동의하는 경우. 다만, 정보주체가 특별한 범주의 개인정보처리 금지원칙을 포기할 수 없다고 유럽연합 또는 회원국의 법률이 규정하는 경우는 예외로 한다.

(b) 적절한 안전장치를 제공하는 유럽연합 또는 회원국의 법률에 의해서 수권을 받는 경우로써 노동법 부문에서 사용자의 의무를 이행하거나 특정한 권리를 행사하는 목적으로 처리되는 경우

(c) 정보주체가 물리적 또는 법률적으로 동의를 할 수 없는 경우로써, 정보주체 또는 다른 사람의 중요한 이익을 보호하기 위해 처리되는 경우

(d) 정치적, 철학적, 종교적 목적을 가지거나 노동조합의 성격을 가진 단체, 재단, 비영리기관이 적절한 안정 장치를 갖추거나 또는 개인정보가 해당 단체의 회원 또는 이전 회원 또는 해당 단체와 정기적으로 접촉하는 사람과 관련해서만 처리된다는 조건과 정보주체의 동의 없이 개인정보를 기관 외부에 공개하지 않는다는 조건을 충족하고 있고 적법한 활동을 수행하는 과정에서 처리하는 경우

(e) 정보주체가 명백히 공개한 개인정보를 처리하는 경우

(f) 소송의 제기, 행사, 방어를 위해 처리하는 경우

(g) 정보주체의 적법한 이익을 보호해 주는 유럽연합 또는 회원국의 법률에 기초하여 공공의 이익을 위한 업무를 수행하기 위해 처리하는 경우

(h) 건강을 위해 그리고 제81조에서 언급한 조건 및 안전 조치에 따라 건강과 관련된 정보를 처리하는 경우

(i) 제83조에서 언급한 조건 및 안전 조치에 따라 역사, 통계, 과학 연구 목적으로 처리되는 경우

(j) 적절한 안전 조치를 제공하는 유럽연합 또는 회원국의 법률에 따라 처리되는 경우로써, 관할기관의 통제 하에 형사재판이나 보안조치와 관련된 정보가 처리되는 경우 또는 개인정보처리자가 준수해야 하는 법률적 의무를 준수하거나 중요한 공익을 위한 업무를 수행하기 위해 처리하는 경우

집행위원회는 1항에서의 규정과 2항의 예외 규정에서 언급한 특정 범주의 개인정보 처리를 위한 기준, 조건, 안전장치를 규정할 목적으로 제86조에 따라 위임된 법안을 채택할 수 있는 권한을 부여 받아야 한다.

제8절 고유식별정보의 처리 제한 (제24조)

1. 현황 및 문제점

개인정보보호법은 '개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.'라고 하여 익명처리의 원칙을 규정하고 있다. 정보주체의 신원이 공개될 경우 사생활 침해 위험이 크고, 특히 주민등록번호와 같은 고유식별정보가 유출·악용될 경우 막대한 경제적 피해까지 우려되기 때문이다. 그러나 현행 개인정보보호법은 정보주체의 별도 동의가 있으면 언제든지 고유식별정보의 수집·이용·제공이 가능하도록 허용함으로써 주민등록번호가 광범위하게 수집·이용되고 있다. 특히 주민등록번호는 거의 모든 개인정보파일 또는 개인정보처리시스템에서 프라이머리 키(primary key, 기본키)로 이용되고 있어 그 자체 빅브라더·빅데이터로써의 역할을 수행하기도 한다.

한편, 정보통신망법은 2012년 2월 17일 법 개정을 통해 정보통신서비스 제공자는 정보주체의 동의가 있는 경우에도 이용자의 주민등록번호를 수집·이용할 수 없게 하고 있어 정보주체의 동의가 있으면 언제든지 고유식별정보의 수집·처리가 가능한 개인정보보호법과 큰 차이를 보이고 있다. 다만, 정보통신망법 제23조의3에 따라 본인확인기관으로 지정받은 경우,

법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우, 영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우에는 예외적으로 주민등록번호의 수집・이용이 가능하지만, 현재로써는 방송통신위원회가 고시한 정보통신서비스 제공자는 없기 때문에 법령에 의하지 않고는 주민등록번호를 수집・이용할 수 없다.

주민등록번호의 수집・이용에 있어서 온라인과 오프라인을 특별히 차별화해야 할 필요성이 없고, 암시장 등을 통해서 거래되고 있는 개인정보의 대부분이 주민등록번호를 확보하기 위한 것이라는 점을 고려한다면 오프라인에서도 온라인에서와 마찬가지로 주민등록번호의 수집・이용과 거래를 하루 빨리 금지해야 한다.

2. 개정방향

고유식별정보는 본인임을 확인하기 위한 식별수단 이외의 목적으로 활용할 수 없게 하여 데이터베이스의 프라이머리 Key 값 등으로 이용하는 것을 금지하고, 고유식별정보를 판매, 대여 등 영리 목적으로 제3자에게 제공, 공유, 공개 등을 할 수 없게 하여 영리목적으로 거래하는 것을 원천적으로 차단하여야 한다. 다만, ‘법령에서 구체적으로 고유식별정보의 처리를

요구하거나 허용하는 경우'에는 고유식별정보를 반드시 본인확인을 위한 식별수단으로만 이용하지 않는 경우도 있으므로 예외를 인정할 필요가 있다. 예컨대 현재 공공기관의 개인정보처리시스템은 대부분 주민등록번호를 프라이머리 Key값으로 활용하고 있다.

정보통신망법과 같이 정보주체의 명시적인 동의가 있더라도 고유식별정보의 수집·이용을 원천적으로 금지하는 방안도 고려할 수 있다. 그러나 이 경우 산업에 미치는 영향이 크고 주민등록번호의 사용에 익숙해 있는 정보주체들(특히 노인 이용자들)도 불편해 할 수 있다. 따라서 먼저 온라인 환경에서 주민등록번호의 수집·이용 없이 거래가 이루어지는 환경에 익숙해지면 점차적으로 오프라인에서도 고유식별정보의 수집을 금지하는 방향으로 가는 것이 바람직할 것이다.

한편에서는 주민등록번호가 전자정부, 전자상거래 등의 발전에 크게 기여했다는 평가를 하며 주민등록번호의 활용을 폭넓게 허용해야 한다고 주장하기도 하나, 전자정부 서비스나 전자상거래는 아이디(ID)/패스워드 기반의 본인확인 절차만으로도 충분하며 그것이 오히려 주민등록번호 기반의 본인확인절차보다 더 안전하다고 할 수 있다.

개정안 신·구 대조표

현 행	개 정 안
제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 “고유식별정보”라 한다)를 처리할 수 없다. 1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우 2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우 <신 설>	제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 “고유식별정보”라 한다)를 처리할 수 없다. 1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우 2. 법률에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우 ② 제1항의 규정에도 불구하고 개인정보처리자는 고유식별정보를 판매, 대여

	등 영리 목적으로 제3자에게 공개 등을 할 수 없고 제1항 제2호의 경우를 제외하고 고유식별정보를 본인임을 확인하기 위한 식별수단 이외의 목적으로 활용할 수 없다.
② 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입할 경우 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.	③ 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입할 경우 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.
③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.	④ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.
④ 행정안전부장관은 제2	

항에 따른 방법의 제공을 지원하기 위하여 관계 법령의 정비, 계획의 수립, 필요한 시설 및 시스템의 구축 등 제반 조치를 마련할 수 있다.	⑤ 행정안전부장관은 제2항에 따른 방법의 제공을 지원하기 위하여 관계 법령의 정비, 계획의 수립, 필요한 시설 및 시스템의 구축 등 제반 조치를 마련할 수 있다.

3. 외국사례

일반적으로 유럽연합, 미국, 일본 등은 공공서비스나 상거래 또는 온라인 활동에 있어서 우리나라에서와 달리 실명과 고유식별정보를 요구하고 있지 아니한다. 주민등록번호 자체가 없는 경우가 많고 납세의무, 사회복지, 운전면허 등을 목적으로 고유식별번호가 부여되기도 하지만, 분야별로 부여되어 있어 오남용 가능성이나 데이터베이스의 프라이머리 키 값으로 사용하기에는 영속성이 부족해 잘 사용되고 있지 않다.

그럼에도 불구하고 미국에서는 사회보장번호(Social Security number ; SSN)가 우리나라에서와 같이 광범위하게 이용되고 있다. 정부기관이나 기업들이 근로자 카드, 의료기록, 건강보험 계좌, 신용 계좌, 은행 계좌, 대학 학생증, 복지시설 등에서 사회보장업무와는 무관하게 사회보장번호가 수집되고 있기 때문

이다. 이에 따라 미국에서도 사회보장번호의 분실, 도용, 상업적 매매가 큰 사회 문제가 되고 있다. 아직까지 사회보장번호의 매매를 금지하거나 수집·이용을 제한하는 연방 법률은 없으나 지난 몇 년 사이에만 사회보장번호의 상업적 매매를 금지하는 법안이 수개나 발의되었다. 그 결과 법률에 의해서 합법적으로 활동하고 있는 대다수 데이터 브로커들이 자율적으로 사회보장번호의 매매 관행을 대폭 축소하고 있다. 또한 일부 주법은 기업이 사회보장번호를 요구하는 것을 제한하거나 사용방법을 규제하기도 한다.[39]

한편 2012년 EU Regulation은 「개인정보처리자가 처리하는 개인정보가 그로 하여금 정보주체의 신원을 확인하도록 허용하고 있지 아니한 경우 개인정보처리자는 개인정보보호법안의 특정 규정을 준수할 목적으로 정보주체의 신원을 확인하기 위해 추가적인 정보를 수집해서는 안 된다」라고 규정하고 있다.[40] 즉 신원확인이 필요하지 아니한 경우에는 신원확인을 위해서는 다른 정보를 수집해서는 안 된다는 것이다.

---

39) Privacy Rights Clearinghouse, My Social Security Number - How Secure Is It?, HTTP://www.privacyrights.org/fs/ fs10-ssn.htm

40) 2012년 EU Regulation 제10조 참조.

제9절 개인정보 영향평가 확대(제33조)

1. 현황 및 문제점

우리나라 개인정보보호법도 개인정보 영향평가제를 도입하고 있으나 영향평가 실시 의무 대상이 공공부문으로 제한되어 있고 주로 대량의 데이터 처리가 예정된 개인정보파일에 한정되어 있다. 따라서 민간부문의 기업들은 대량의 개인정보처리시스템을 도입하거나 확대하면서도 영향평가를 받아야 할 필요가 없어 개인정보보호가 사전예방보다는 사후구제조치에 머물고 있다.

물론 민간 기업들의 경우 정보통신망법에 따른 정보보호관리체계인증(ISMS)이나 개인정보관리체계인증(PIMS)을 통해 개인정보파일이나 개인정보처리시스템의 취약점을 발견할 수 있으나 이들 평가·인증시스템은 임의제도이기 때문에 인증이 의무화 되어 있지 않다. 따라서 극히 소수의 기업들만이 정보보호관리체계인증(ISMS)이나 개인정보관리체계인증(PIMS)을 받고 있다.

2. 개정방향

영향평가 실시 의무 대상을 공공부문에서 민간부문으로까지 확대하고, 유전자정보 등 민감정보가 포함된 개인정보파일의 경우 대량의 데이터 처리가 예정되어 있지 아니한 경우에도 영향평가 실시 의무 대상에 포함하도록 하여야 한다. 특히 빅데이터 시스템, 클라우드 컴퓨팅, SNS, USN(Ubiquitous Sensor Network), 비디오감시 시스템, 바이오인식 시스템, 각종 평가시스템 등을 영향평가 대상에 포함하여야 한다.

그러나 영향평가제를 도입하고 있는 나라 중 영향평가를 지정된 외부기관에만 의뢰하도록 하고 있는 나라는 찾기 어렵다. 포괄적인 영향평가제를 도입한 2012년 EU Regulation도 영향평가의 대상, 방법, 절차에 대해서만 규정하고 있을 뿐이다. 다른 나라의 경우 오히려 영향평가는 내부적으로 이루어지는 경우가 많다. 따라서 민간부문에서의 영향평가는 하위법령에서 정한 기준, 방법, 절차 등에 따라 사업자들이 자율적으로 판단해서 하도록 한 것이다. 영향평가는 서비스나 시스템 개발 단계에서 이루어지기 때문에 이를 외부 기관에 의뢰할 경우 민간기업의 경우 신제품 관련 영업비밀이 유출될 수 있는 등 문제가 발생할 수 있다. 다만, 공공기관의 경우에는 영업비밀 등의 유출 위험이 없고 현재도 행정안전부가 지정한 평가기관에서 하도록 하고 있으므로 이를 그대로 인정한 것이다.

개정안 신·구 대조표

현 행	개 정 안
제33조(개인정보 영향평가) ① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 “영향평가”라 한다)를 하고 그 결과를 행정안전부장관에게 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 행정안전부장관이 지정하는 기관(이하 “평가기관”이라 한다) 중에서 의뢰하여야 한다.	제33조(개인정보 영향평가) ① 개인정보처리자는 개인정보처리의 특성, 범위, 목적 등으로 인해 해당 개인정보파일이 정보주체의 권리와 자유를 침해할 위험이 있는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 그 위험요인의 분석과 개선 사항을 도출하기 위한 평가(이하 “영향평가”라 한다)를 하여야 한다. 1. 개인의 특성, 경제적 상황, 위치, 건강, 개인적 선호, 신뢰도, 품행 등을 자동적으로 분석·예측하기 위하여 구축한 체계적인

	평가시스템 2. 특정 개인에 대한 조치나 결정을 내리기 위해 민감정보를 처리하는 개인정보처리시스템 3. 비디오 감시 시스템 등 공개된 장소에 대한 모니터링 시스템 4. 어린이에 관한 정보, 바이오 인식정보를 포함하고 있는 파일링시스템 5. 그 밖에 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우로써 대통령령으로 정하는 기준에 해당하는 경우
② 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다. 1. 처리하는 개인정보의 수 2. 개인정보의 제3자 제공 여부 3. 정보주체의 권리를 해할 가능성 및 그 위험 정도	② 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다. 1. 처리하는 개인정보의 수 2. 개인정보의 제3자 제공 여부 3. 정보주체의 권리를 해할 가능성 및 그 위험 정도

4. 그 밖에 대통령령으로 정한 사항	4. 그 밖에 대통령령으로 정한 사항
<신 설>	③ 공공기관이 제1항에 따라 영향평가를 하고자 하는 때에는 행정안전부장관이 지정하는 기관(이하 “평가기관”이라 한다) 중에서 의뢰하여야 하고, 평가결과를 행정안전부장관에게 제출하여야 한다.
③ 행정안전부장관은 제1항에 따라 제출받은 영향평가 결과에 대하여 보호위원회의 심의·의결을 거쳐 의견을 제시할 수 있다.	③ 행정안전부장관은 제1항에 따라 제출받은 영향평가 결과에 대하여 보호위원회의 심의·의결을 거쳐 의견을 제시할 수 있다.
④ 공공기관의 장은 제1항에 따라 영향평가를 한 개인정보파일을 제32조제1항에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다.	④ 공공기관의 장은 제1항에 따라 영향평가를 한 개인정보파일을 제32조제1항에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다.
⑤ 행정안전부장관은 영향평가의 활성화를 위하여 관계 전문가의 육성, 영향평가 기준의 개발·보급 등	⑤ 행정안전부장관은 영향평가의 활성화를 위하여 관계 전문가의 육성, 영향평가 기준의 개발·보급 등

필요한 조치를 마련하여야 한다.	필요한 조치를 마련하여야 한다.
⑥ 제1항에 따른 평가기관의 지정기준 및 지정취소, 평가기준, 영향평가의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.	⑦ 제1항에 따른 세부적인 평가대상 기준, 평가 방법 및 절차 등에 관하여 필요한 사항과 제3항에 따른 평가기관의 지정기준 및 지정취소 등에 관하여 필요한 사항은 대통령령으로 정한다.
⑦ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따른다.	⑧ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따른다.
⑧ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.	<삭 제>

3. 외국사례

아직 민간부문에 대해서까지 개인정보 영향평가를 의무화하고 있는 나라는 많지 않다. 개인정보 영향평가를 법적으로 또는 정책적으로 의무화 하고 있는 나라로는 캐나다, 미국, 홍콩, 영국, 호주, 뉴질랜드 등 6개국이다. 캐나다는 2002년 세계에서 최초로 공공부문에 대한 개인정보 영향평가를 의무화 하였고,[41] 이어 미국도 공공부문에 대한 개인정보 영향평가를 의무화 하였다.[42] 그러나 이들 두 나라는 민간부분에 대해서 개인정보 영향평가를 의무화 하고 있지 않다. 유럽연합은 공공부문과 민간부문을 구분하지 않고 RFID에 대한 영향평가를 권고하고 있다. 영국은 2007년 12월에 유럽연합 회원국 중 개인정보 영향평가제도를 도입한 최초의 국가이다. 그러나 이는 법적으로 의무화 되어 있는 것은 아니고 영국 개인정보보호기구(ICO)의 권고 사항일 뿐이다. 다만 공공부문에 대하여는 사실상 의무화되어 있다.[43]

그러나 2012년 유럽연합 집행위원회가 발표한 2012년 EU Regulation은 민간부문과 공공부문 전체에 대해서 개인정보

41) 캐나다 Privacy Act 제3조 및 Treasury Board of Canada Secretariat(TBS)의 Directive on Privacy Impact Assessment (effective April 1, 2010) 참조.

42) 미국 E-Government Act of 2002 참조.

43) David Wright, Should privacy impact assessments be mandatory?, Communications of the ACM, Vol. 54, No. 8, August 2011. http://www.trilateralresearch.com

영향평가를 의무화 하고 있다.[44] 즉 개인정보처리의 특성, 범

44) 2012년 EU Regulation 제33조 참조. Article 33(Data protection impact assessment) 1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
2. The following processing operations in particular present specific risks referred to in paragraph 1: (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual; (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale; (c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale; (d) personal data in large scale filing systems on children, genetic data or biometric data; (e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).
3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.
4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.
5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4

위, 목적 등으로 인하여 개인정보를 처리하는 과정에 정보주체의 권리와 자유가 위협받을 위험이 있는 경우 개인정보처리자 또는 개인정보처리자를 대신하여 개인정보를 처리하는 자는 예상되는 처리과정이 개인정보보호에 미치는 영향을 평가하여야 한다. 특히 다음 각 호의 경우에는 개인정보처리 활동이 정보주체의 권리와 자유에 특별한 위협을 유발할 위험이 있는 것으로 본다.

a) 자동화된 처리에 기초하여 개인에게 법적 효과를 유발하거나 중대한 영향을 미칠 수 있는 평가시스템으로써, 자연인의 사적인 측면을 평가하거나 자연인의 경제적 상황, 위치정보, 건강상태, 개인적 선호, 신뢰도, 품행(행태) 등을 분석하거나 예측하기 위한 체계적이고도 광범

---

shall not apply, unless Member States deem it necessary to carryout such assessment prior to the processing activities.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and autostability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.

7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

위한 평가

(b) 특정한 개인을 대상으로 대규모의 조치를 취하거나 결정을 내리기 위해 성생활, 건강, 인종, 출신 민족, 건강보험제공, 전염병연구, 정신병·전염병의 조사 등에 관한 정보개인정보가 처리되는 경우

(c) 공개적으로 접근 가능한 지역을 감시하는 경우 특히 광전자 장치(비디오 감시 카메라)를 대규모로 사용하는 경우

(d) 대규모의 파일링시스템(filing system)에 들어 있는 어린이 관련정보, 유전자정보, 생체인식정보 등의 개인정보

(e) 그 밖에 정보주체의 권리와 자유에 대한 위험이 커서 제34조 (2)항 (b)에 따라 개인정보보호기구의 특별한 사전 컨설팅이 필요한 처리

제10절 개인정보 유출 통지·신고 의무 강화 (제34조제3항)

1. 현황 및 문제점

개인정보보호법은 개인정보유출 사고 시 정보주체에 대한 통지의무를 부과하고 있으나 정보주체의 연락처를 알지 못한 경우에 대한 규정이 미비하다. 이에 따라 유출사고가 발생했음에도 불구하고 정보주체의 연락처를 모른다는 이유로 통지의무를 회피하거나 늑장을 부리는 사례가 발생하고 있다. 또한, 개인정보보호법은 유출사고 발생 시 피해의 확산과 확대를 신속하게 방지하게 하기 위하여 선 보호조치를 하고 후 결과보고를 하도록 하고 있고, 개인정보처리자들이 보고에 필요한 조치들을 준비할 수 있도록 표준 개인정보보호지침에 의하여 5일간의 신고유예기간을 주고 있으나, 이와 같은 선 조치 후 보고 제도를 악용하여 책임을 회피할 구실을 찾는데 시간을 보내고 있다.

이에 반하여 정보통신망법은 「정보통신서비스 제공자등이 개인정보의 분실·도난·누출(이하 "누출 등"이라 한다) 사실을 안 때에는 지체 없이 일정 사항을 해당 이용자에게 알리고 방송통신위원회에 신고하여야 한다.」라고 하여 선 신고 후 보고

원칙을 채택하고 있다. 또한 정보통신서비스 제공자등이 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있도록 대체적인 방법을 마련해 두고 있다.[45]

2. 개정방향

개인정보처리자의 책임 없는 사유로 정보주체의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 신속하게 통지에 갈음하는 조치(홈페이지, 신문·방송 등 공개)를 취하도록 의무화 하여야 하나다. 또한, 선 보호조치 후 결과보고 제도를 선 보고조치 후 보호조치 원칙으로 전환하고, 유출사고가 발생한 때에는 관련기관에 대한 신고를 “24시간 내”에 하도록 하여 신속한 사고조사와 피해예방이 동시에 이루어지도록 하여야 한다.

선 보고조치 원칙을 채택할 경우 개인정보처리자들이 피해예방이나 확산방지 노력은 하지 않고 보고서 준비에 시간을 보내게 될 것이라는 우려가 있을 수 있으나, 유출사실을 알게 되었을 때에는 24시간 내에는 대통령령이 정하는 바에 따라 알고 있는 사실만 그대로 신고하면 되고 아직 확인되지 아니한 신고사항에 대하여는 추후에 신고할 수 있게 함으로써 신

45) 정보통신망법 제27조의3 참조.

고 준비를 빙자하여 피해예방 및 피해확산방지 의무를 소홀히 하지 못하도록 하면 될 것이다.

한편, 개인정보보호법 제34조제3항은 대통령령으로 정한 규모 이상(현행 1만 명)의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고하도록 하고 있으나 1만 명 이하의 유출 사건에 대해서는 신고의무가 없다. 그러나 유사사례방지 등을 위해 특정 사건의 경우에는 정부가 관련 정보를 알아야 할 필요가 있을 수 있으므로 행정안전부장관이 요구한 경우에는 '조치결과'를 제출하게 할 필요가 있다. 다만, 제출의무를 지나치게 확대하면 사적 자치를 침해할 우려가 있으므로 제출 대상을 사후적인 '조치결과'로 제한하고 제출의무도 일반화하지 않고 정부가 필요한 경우로 한정하였다.

개정안 신·구 대조표

현 행	개 정 안
제34조(개인정보 유출 통지 등) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체	제34조(개인정보 유출 통지 등) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체

없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.	없이 해당 정보주체에게 다음 각 호의 모든 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.
1. 유출된 개인정보의 항목	1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위	2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보	3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차	4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처	5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
② 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.	② 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 하며 행정안전부장관의 요구가 있는

	경우 그 조치결과를 제출하여야 한다.
③ 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 행정안전부장관 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.	③ 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항 각 호의 모든 사항을 24시간 내에 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 행정안전부장관 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.
④ 제1항에 따른 통지의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.	④ 제1항 및 제3항에 따른 통지 및 신고의 시기, 방법, 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

3. 외국사례

개인정보침해에 대한 통지 및 신고 제도는 미국 캘리포니아 주법에서 최초로 도입되었다. 이것이 점차 다른 주로 확대되어

최근에는 상당수의 주들이 개인정보침해에 대한 통지 및 신고 제도를 도입하고 있다. 2012년 9월 현재 앨라배마, 켄터키, 뉴멕시코, 사우스다코타 등을 제외한 대다수 들이 개인정보침해 신고 제도를 도입하고 있다.

캘리포니아 주법을 예로 들어 보면 개인정보처리자는 침해사실의 공개가 수사기관의 수사를 방해하지 않는 한 지체 없이(without unreasonable delay) 그리고 가장 편리한 시간 내에 피해를 입은 정보주체에게 문서 또는 전자문서로 통지를 해야 한다. 다만 침해규모가 매우 큰 경우에는 법률이 정하는 바에 따라 개별적인 통지에 갈음하여 신문 공고 등으로 대체할 수 있다. 일반적인 개인정보 침해 사고에 대하여는 주 당국에 신고할 의무가 없지만, 의료정보나 건강정보가 침해를 받은 경우에는 5일 이내에 주 당국에 신고하여야 하고, 500명 이상의 개인정보가 침해를 받은 경우에는 캘리포니아 주 검찰총장에게 신고하여야 한다.[46] 다만, 분실, 도난, 유출된 개인정보가 암호화 되어 있는 경우에는 통지·신고 의무는 적용되지 아니한다. 정보주체는 통지를 받을 권리를 포기할 수 없다.

한편, 2012년 EU Regulation은 미국보다는 좀 엄격한 개인정보침해 통보 및 신고 제도를 도입하고 있다.[47] 개인정보처리자

46) 미국은 주마다 개인정보침해 신고·통지제도가 상당히 다르다. 예컨대 애리조나 주 같은 경우에는 개인정보처리자나 법집행기관이 합리적인 조사를 하고 나서 해당 침해사고가 정보주체의 권리침해를 가져오지 않을 것으로 판단한 경우에는 정보주체에게 개별적인 통지를 하지 않아도 된다.

는 개인정보가 침해를 받은 경우에는 침해사실을 알게 된 때부터 가능한 한 24시간 이내에 지체 없이 침해 사실을 개인정보보호기구에 신고하여야 한다. 만약 개인정보보호기구에 24시간 이내에 통지하지 않거나 못한 경우에는 그에 대한 합당한 이유를 신고에 포함시켜야 한다. 개인정보를 취급하는 취급자(수탁자 등)는 개인정보의 침해 사실을 확인한 후에는 즉시(immediately) 개인정보처리자에게 그 사실을 보고하여야 한다. 개인정보보호기구에 신고하는 신고서에는 최소한 다음 각 호의 모든 사항에 포함되어야 한다.

(a) 관련된 정보주체의 범주 및 수와 관련된 개인정보의 범주 및 수를 포함하여 개인정보 침해의 특성에 대한 설명

(b) 정보보호 담당자의 신원 및 상세 연락처 그리고 더 많은 정보를 얻을 수 있는 경우에는 다른 사람의 신원 및 상세 연락처

(c) 개인정보 침해의 부정적인 효과를 완화하기 위해 권고되는 조치

(d) 개인정보 침해로 인해 발생할 수 있는 결과에 대한 설명

(e) 개인정보 침해 문제를 처리하기 위해 개인정보처리자가

47) 2012년 EU Regulation 제31조 참조.

제안하거나 취한 조치에 대한 설명

개인정보처리자는 개인정보침해를 문서화해야 한다. 해당 문서에는 침해와 관련된 사실(facts) 및 그 결과 그리고 구제조치 등이 포함되어야 한다. 또한 해당 문서는 개인정보보호기구가 이를 통해서 규정의 준수 여부를 확인할 수 있도록 작성되어야 한다.

또한 개인정보침해로 인해 개인정보보호나 정보주체의 프라이버시보호에 부정적인 영향을 미칠 것으로 예상되는 경우 개인정보처리자는 제31조에 따라 개인정보보호기구에 침해 사실을 통지한 후 지체 없이(without undue delay) 개인정보 침해 사실을 정보주체에게 알려야 한다.[48] 개인정보처리자가 정보주체에게 침해사실을 통지하지 아니한 경우 개인정보 침해 사실을 정보주체에 통지해야 하는 개인정보처리자의 의무를 침해함이 없이 개인정보보호기구는 침해로 인해 예상되는 부정적인 효과를 고려하여 개인정보처리자에게 정보주체에 대한 통지의무를 이행하도록 명할 수 있다. 그러나 만약 개인정보처리자가 기술적인 보호 조치를 적절하게 취하였고 그와 같은 조치가 침해받은 정보에 적절하게 적용되었다는 것을 개인정보보호기구가 만족할 수 있을 정도로 입증한 경우에는 개인정보

48) 2012년 EU Regulation 제32조 참조.

침해 사실을 정보 주체에 알리지 않아도 된다. 여기서 말하는 기술적 보호조치란 해당 정보에 접근할 수 없는 사람들이 그 정보를 알아 볼 수 없도록 하는 것을 의미한다.

제11절 제3자 제공한 개인정보에 대한 파기조치의무(잊혀 질 권리) 신설 등 (제36조, 제37조)

1. 현황 및 문제점

개인정보보호법은 개인정보 처리정지 요구권을 규정하면서도 동의 철회권에 대해서는 명확한 규정을 두고 있지 아니한다. 이에 따라 실무에서는 정보주체가 개인정보처리에 동의를 한 경우에는 개인정보처리 동의 철회를 요구할 수 없고, 공개된 정보 등으로부터 수집한 개인정보에 대해서만 처리정지 요구가 가능하다는 해석이 이루어지고 있기도 한다.

또한, 정보주체는 개인정보처리자에게는 자신의 개인정보에 대한 처리 정지를 요구할 수 있는 처리정지 요구권을 가지고 있지만, 개인정보처리자가 제3자에게 제공한 개인정보에 대해서는 개인정보 자기통제권을 행사하는 것이 현실적으로 곤란하다. 정보주체는 개인정보처리자로부터 자신의 개인정보를 제공받은 제3자를 알기 어렵고, 알고 있다고 해도 일일이 처리정

지를 요구하는 것은 시간적·경제적으로 한계가 있다.

2. 개정방향

다른 사람과 소통하고 싶은 권리만큼이나 숨기고 싶은 자신의 과거로부터 벗어나고자 하는 '잊혀 질 권리'의 보장도 중요하다. 먼저 해석상의 혼란을 피하기 위해 현행법상 인정되고 있는 개인정보 처리정지 요구권 이외에 동의 철회권을 개인정보보호법에 명시적으로 규정하여야 한다. 정보통신망법에서는 「이용자는 정보통신서비스 제공자등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있다.」라고 규정하고 있다.[49)]

또한 정보주체가 동의철회 또는 처리정지 요구를 해 온 경우 개인정보처리자는 제3자에 대한 개인정보의 제공·공유 등을 즉시 중단하고 자신이 정보주체의 개인정보를 제공·공유하였거나 제공·공유하고 있는 제3자에게 정보주체로부터 개인정보처리에 대한 동의철회 또는 처리정지 요구가 들어왔음을 알리고 제공받은 개인정보를 지체 없이 삭제·파기 또는 반환하도록 조치하여야 한다.

그러나 개인정보처리자가 정보주체의 동의를 받거나 법률상

49) 정보통신망법 제30조제1항 참조. 비슷하게 정보통신망법에는 개인정보처리정지 요구권이 규정되어 있지 아니하여 해석상 논란이 있다.

정당한 근거에 기해서 제3자에게 제공한 개인정보에 대해서까지 삭제·파기 등의 책임을 지라는 것은 가혹하다는 비판이 있을 수 있다. 오히려 개인정보처리자가 일괄적으로 제3자에 대하여 정보주체에 관한 개인정보를 파기·삭제하도록 조치할 경우 정보주체가 예상하지 못한 피해를 입을 수도 있다는 주장도 가능하다. 하지만 개인정보처리자가 조치를 취해야 할 제3자의 범위, 유형 등은 대통령령으로 합리적으로 제한하면 되고 일괄 삭제·파기에 따른 정보주체는 제휴 서비스를 제외하면 예상하기 어려우므로 크게 문제되지 아니할 것으로 보인다. 더구나 대부분의 개인정보 제3자 제공이 정보주체의 필요에 의해서보다는 개인정보처리자의 필요에 의해서 이루어지고 있는 현실을 고려한다면 제3자 제공을 통해 이익을 보고 있는 개인정보처리자가 그 정도의 비용과 노력은 감수하여야 할 것이다.

개정안 신·구 대조표

현 행	개 정 안
제37조(개인정보의 처리정지 등) ① 정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다. 이 경우	제37조(개인정보의 처리정지 등) ① 정보주체는 개인정보처리자에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회하

공공기관에 대하여는 제32조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다.	거나 수집·이용·제공 등의 정지(이하 이 조에서 “처리정지”라 한다)를 요구할 수 있다. 이 경우 공공기관에 대하여는 제32조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다.
② 개인정보처리자는 제1항에 따른 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다. 1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 2. 다른 사람의 생명·신체	② 개인정보처리자는 제1항에 따른 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 동의철회 또는 처리정지 요구를 거절할 수 있다. 1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 2. 다른 사람의 생명·신체

를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우	를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우	3. 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우
4. 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우	4. 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우
③ 개인정보처리자는 제2항 단서에 따라 처리정지 요구를 거절하였을 때에는 정보주체에게 지체 없이 그 사유를 알려야 한다.	③ 개인정보처리자는 제2항 단서에 따라 동의철회 또는 처리정지 요구를 거절하였을 때에는 정보주체에게 지체 없이 그 사유를 알려야 한다.
④ 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인	④ 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인

정보의 파기 등 필요한 조치를 하여야 한다.	정보의 파기 등 필요한 조치를 하여야 한다. 이 경우 제3자에게 제공(공유·공개를 포함한다)된 개인정보가 있으면 개인정보처리자는 지체 없이 대통령령이 정하는 방법으로 정보주체로부터 동의철회 또는 처리정지를 요구받은 사실이 있었음을 알리거나 공개하고 해당 정보가 삭제·파기되도록 조치하여야 한다.
⑤ 제1항부터 제3항까지의 규정에 따른 처리정지의 요구, 처리정지의 거절, 통지 등의 방법 및 절차에 필요한 사항은 대통령령으로 정한다.	⑤ 제1항부터 제3항까지의 규정에 따른 동의철회 또는 처리정지의 요구 및 거절, 거절사유 통지 등의 방법 및 절차에 필요한 사항은 대통령령으로 정한다.

3. 외국사례

2012년 EU Regulation은 이른바 '잊혀 질 권리'(Right to

forgotten)의 하나로 개인정보처리자에게 제3자에 대해서도 일정한 범위의 조치의무를 부담하도록 규정하고 있다.[50] 즉, 개인정보처리자는 자신의 책임 하에서 개인정보를 공개한 경우 공개된 개인정보를 처리하고 있는 제3자에게 정보주체가 해당 정보의 링크·복제·복사의 제거를 요구해 왔음을 알리기 위하여 기술적인 조치를 포함하여 모든 합리적인 조치를 취하여야 한다. 또한 개인정보처리자가 제3자에게 개인정보의 공개(발표)를 허락한 경우에는 그 공개에 대해서도 책임을 지는 것으로 간주한다(제17조제2항). 지금까지는 정보주체의 권리가

50) 2012년 EU Regulation 제17조 참조. Article 17(Right to be forgotten and to erasure) 1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
(c) the data subject objects to the processing of personal data pursuant to Article 19;
(d) the processing of the data does not comply with this Regulation for other reasons.
2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorized a third party publication of personal data, the controller shall be considered responsible for that publication.

개인정보처리자에 대한 권리로 한정되어 있었지만, 개인정보처리자가 개인정보를 제공한 제3자에게로까지 확대된 것이다. 이와 같은 권리와 의무를 모두 합해서 EU에서는 잊혀 질 권리라 부르고 있으며 빅데이터와 클라우드컴퓨팅 시대에 있어서 매우 중요한 권리로 여겨지고 있다.

잊혀 질 권리에 대한 한·EU 간 비교

잊혀 질 권리의 주요내용	2012 EU Regulation	개인정보보호법	정보통신망법
부정확한 정보의 정정요구권	○	○	○
개인정보 삭제 요구권	○	○	○
삭제 대상 정보의 확산방지 의무	○	×	×
개인정보 처리 정지 요구권	○	○	△ (동의철회권)
삭제에 갈음한 개인정보의 처리 제한	○	×	×
링크·복제·복사의 중단·삭제 통지의무	○	×	×
개인정보 유효기간제	×	×	○
사생활 침해정보 등 삭제요청권	×	×	○

제12절 개인정보 복제·이전 청구권 신설 (제37조의2)

1. 현황 및 문제점

개인정보보호법은 정보주체에게 자신의 개인정보에 대한 열람을 요구할 수 있는 권리는 부여하고 있다(제35조제1항). 그러나 자신에 관한 모든 정보의 사본을 제공해 달라거나 자신이 지정한 다른 개인정보처리자에게 해당 정보를 이전해 달라고 요구할 수 있는 권리는 인정되지 않고 있다. 이에 따라 특정 개인정보처리자의 정보시스템 내에 정보주체의 일상과 추억이 쌓이고 가치 있는 정보가 축적되면 정보주체는 해당 개인정보처리자가 제공하는 서비스에 더욱 종속하게 되고 자신의 개인정보에 대한 통제권 행사가 더욱 어려워지게 된다.

최근 개인정보처리자의 정보 저장능력이 획기적으로 향상되고 사회관계망서비스의 이용이 급증함에 따라 특정 개인정보처리자에 대한 정보주체의 의존도가 날로 심화되고 있는 현실에서 정보주체는 개인정보처리자가 제공하는 서비스에 평생 동안 종속되어 있거나 개인정보처리자가 보유하고 있는 자신에 관한 정보를 모두 포기해야 하는 양자택일을 강요받고 있다.

2. 개정방향

정보주체가 특정 개인정보처리자의 노예가 되지 않도록 개인정보처리자의 정보시스템 내에 저장되어 있는 자신에 관한 개인정보를 언제든지 전자적인 형태로 이전받을 수 있는 권리를 보장(Right to data portability)하여야 한다. 이는 사회관계망서비스(SNS), 클라우드컴퓨팅서비스, 온라인쇼핑몰 등 각종 온라인 거래 및 활동에 있어서 회원 탈퇴 및 이전의 자유를 보장함으로써 정보주체의 권리 보호는 물론, 사업자 간 서비스 경쟁을 유도할 수 있는 긍정적 효과도 기대할 수 있다.

최근 사회관계망서비스나 클라우드컴퓨팅서비스 등을 제공하고 있는 일부 외국계 기업들은 자발적으로 웹사이트 상에서 정보주체가 언제든지 자신에 관한 정보를 내려받기해 갈수 있도록 하여 개인정보의 복제청구권을 보장하고 있다. 자신에 관한 정보를 다른 서비스제공자에게 그대로 이전해 달라고 요구할 수 있는 정보의 이전청구권까지 보장하기 위해서는 서비스의 표준화 등 해결해야 할 선결과제가 많겠지만, 일반적으로 많이 사용하는 전자적 형식으로 전환하여 다른 사람에게 이전시키거나 전송하는 것은 충분히 가능할 것이다.

정보주체가 복제 또는 이전을 요구할 수 있는 개인정보의 범위에 대해서 논란이 있을 수 있으나 요구 대상정보는 정보주체가 제공하거나 게시한 개인정보로 한정하여야 할 것이다. 개

인정보처리자가 정보주체 이외로부터 수집한 개인정보나 개인정보처리자가 생성·생산한 개인정보는 정보주체에 관한 개인정보라 할지라도 정보주체의 정보는 아니고 또한 그와 같은 정보는 정보주체에게 보존 또는 소장의 가치가 있을 만큼 중요한 정보로 보기는 어려울 것이다. 따라서 복제·이전의 대상은 사진, 댓글, 메시지, 주소록, 연락처 등 정보주체에게 역사적 가치가 있거나 사회·경제적 필요가 있는 정보로 한정하여야 한다.

개정안 신·구 대조표

현 행	개 정 안
<신 설>	제37조의2(개인정보의 이전·복제 요구) ① 정보주체는 자신이 제공한 개인정보를 개인정보처리자가 정보통신망을 통하여 전자적으로 보관하고 있는 경우에는 언제든지 복제를 요구할 수 있고 개인정보처리시스템(개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시

	스템을 말한다)을 통하여 보관하고 있는 경우에는 다른 개인정보처리자의 개인정보처리시스템으로 이전을 요구할 수 있다. ② 개인정보처리자는 개인정보의 복제·열람으로 인해 비용이 소요되는 경우에는 대통령령이 정하는 바에 따라 실비의 범위 내에서 수수료와 우송료를 청구할 수 있다. 다만, 정보주체가 정보통신망을 통해 자신의 저장매체에 직접 개인정보를 복제하거나 내려받기를 한 경우에는 그러하지 아니한다. ③ 제1항에 따라 정보주체가 이전 또는 복제를 요구할 수 있는 개인정보의 범위 또는 대상은 대통령령으로 정한다.

3. 외국사례

정보 복제 및 이전 청구권은 클라우드컴퓨팅서비스, 사회관계망서비스 등이 현실화되고 이용자가 확대되면서 비교적 최근에 이슈화된 문제로 법제화된 해외의 사례를 찾기는 어렵다. 다만, 국내에서는 방송통신위원회가 준비 중인 가칭 '클라우드 컴퓨팅 서비스 발전법안'에서 정보 복제 및 이전 청구권을 규정하고 있다. 유럽연합 개인정보보호법안에서도 전자적 수단에 의해 처리되는 정보에 대한 사본 요구권과 이전 요구권을 규정하고 있다.[51] 동 법안은 「개인정보가 전자적 수단에 의해서 체계적이고 일반적으로 많이 사용되는 형식으로 처리되고 있는 경우 정보주체는 일반적으로 많이 사용되고 추후에 계속해서 사용할 수 있는 전자적 형식으로 자신에 관한 정보의 복사본을 개인정보처리자에게 요구할 권리를 가진다.」라고 규정하는 한편, 「정보주체가 개인정보를 제공하였고 개인정보의 처리가 동의나 계약에 근거해서 이루어지고 있는 경우 정보주체는 자신이 제공하고 개인정보처리자의 자동화된 처리 시스템이 보관하고 있는 개인정보를 일반적으로 많이 사용하는 전자적 형식으로 다른 사람에게 전송해 줄 것을 개인정보처리자에게 요구할 수 있는 권리를 가진다.」라고 규정하여 복제요구권과 이전요구권을 명시적으로 인정하고 있다. 또한, 유럽연합 집행위원회로 하여금 본조에서 언급된 '전자적 형식', 개인정보

51) 2012년 EU Regulation 제18조 참조.

의 전송을 위한 기술 표준, 형식, 절차 등에 대해서 규정할 수 있도록 하고 있다.

제13절 열람권·거부권 등 권리행사 용이화(제38조의2)

1. 현황 및 문제점

개인정보보호법은 정보주체에게 자신의 개인정보에 대한 열람요구권(제35조), 정정·삭제요구권(제36조), 처리정지요구권(제37조) 등을 인정하고 있다. 이 경우 개인정보처리자는 개인정보처리자를 직접 방문하거나 우편 등으로 요구해야 하고 관련 비용(수수료와 우송료)도 납부해야 한다. 이에 따라 권리행사에 많은 시일이 소요될 뿐만 아니라, 경제적·인력적 낭비도 심하다. 따라서 많은 정보주체들이 자신의 권리행사를 포기해 버려 정보주체의 권리가 유명무실한 종이호랑이가 되어 버리고 있다.

2. 개정방향

정보주체가 개인정보 자기통제권을 행사할 수 있도록 개인정

보에 대한 일정한 권리를 부여하는 것도 중요하지만, 그 권리를 편리하고 쉽게 행사할 수 있게 하는 것도 국가의 책무라고 할 수 있다.

따라서 발달된 정보통신환경을 고려하여 개인정보처리자가 개인정보를 정보통신망을 통해 전자적으로 처리하는 경우에는 정보주체가 개인정보처리자의 손을 빌리지 않고 해당 정보통신망을 통해서 열람, 정정·삭제, 처리정지 등의 권리를 직접 행사할 수 있는 조치 또는 수단을 마련해 제공하도록 하여야 한다. 아울러 이 경우에는 정보주체에게 수수료, 우송료 등을 청구할 수 없도록 해야 한다.

현재 대다수 온라인 기업들이 웹사이트 상에서 '나의 개인정보관리' 등의 코너를 마련하여 열람, 정정·삭제, 처리정지 등의 권리를 행사할 수 있는 서비스를 제공하고 있지만, 개인정보의 목적 외 이용 및 제3자 제공에 관한 내역은 제공하고 있지 않다. 또한, 일부 기업은 이와 같은 서비스 자체를 제공하고 있지 않기 때문에 이를 법제화 하여 정보주체의 권리행사를 용이하게 할 필요가 있다.

개정안 신·구 대조표

현 행	개 정 안
제38조(권리행사의 방법 및 절차) ① 정보주체는 제35	제38조(권리행사의 방법 및 절차) ① 정보주체는 제

조에 따른 열람, 제36조에 따른 정정·삭제, 제37조에 따른 처리정지 등의 요구(이하 “열람 등 요구”라 한다)를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다.	35조에 따른 열람, 제36조에 따른 정정·삭제, 제37조에 따른 처리정지, 제37조의2에 따른 이전·복제 등의 요구(이하 “열람 등 요구”라 한다)를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다.
② 만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보 열람 등 요구를 할 수 있다.	② 만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보 열람 등 요구를 할 수 있다.
③ 개인정보처리자는 열람 등 요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구할 수 있다.	③ 개인정보처리자는 열람 등 요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구할 수 있다. 다만, 제4항의 경우에는 그러하지 아니한다.
<신 설>	④ 개인정보처리자는 개인정보를 정보통신망을 통해 전자적으로 처리하는 경우

	에는 정보주체가 해당 정보통신망을 통해서 열람, 정정·삭제, 처리정지 등의 권리를 직접 행사할 수 있도록 조치하여야 한다. 다만, 법령 등에 의하여 열람 등의 요구를 거절할 수 있는 경우에는 그 사유를 밝히고 조치 대상에서 제외할 수 있다.
④ 개인정보처리자는 정보주체가 열람 등 요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.	⑤ 개인정보처리자는 정보주체가 열람 등 요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 개인정보처리방침에 공개하여야 한다.
⑤ 개인정보처리자는 정보주체가 열람 등 요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.	⑥ 개인정보처리자는 정보주체가 열람 등 요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

3. 외국사례

정보주체가 자신의 권리를 전자적인 방법으로 행사할 수 있게 하도록 개인정보처리자에게 의무를 부여하고 있는 해외 법률은 아직 발견하기 어렵다. 다만, 2012년 EU Regulation은 정보주체가 전자적인 방식으로 권리를 행사해 온 경우 정보주체가 달리 요청하지 않는 한 전자적인 방식으로 정보를 제공할 수 있게 하고 있다.[52] 그러나 이는 정보주체가 전자적 방식으로 요구하면 전자적 방식으로 답변하면 된다는 것일 뿐 정보주체가 개인정보처리자의 손을 빌리지 않고 온라인상에서 스스로 권리를 행사할 수 있는 방법은 아니다.

제14절 단체소송의 조정전치주의 폐지(제51조)

1. 현황 및 문제점

개인정보 유출과 오남용으로 인한 피해는 집단적인 경우가 많다. 따라서 개인정보보호법은 각종 개인정보 침해행위로부터 정보주체의 권리를 신속·간편하게 구제하기 위하여 단체소송

52) 2012년 EU Regulation 제12조제2항 후단 참조.

제도를 도입하고 있다. 그런데 개인정보보호법은 개인정보 단체소송제도를 도입하면서 조정전치주의를 채택하고 있다. 즉 개인정보침해를 이유로 단체소송을 제기하려면 반드시 먼저 집단분쟁 조정절차를 거쳐야 한다. 개인정보피해는 신속한 구제조치가 필요한 경우가 많음에도 불구하고 조정전치주의의 도입으로 인해 단체소송제도 도입의 취지를 살리기 어렵게 되었고 분쟁상태의 장기화를 초래할 가능성만 커졌다.

한편, 개인정보 단체소송제도는 소비자기본법상 소비자 단체소송제도를 모델로 하고 있으나 소비자 보호단체와 개인정보 보호단체는 여러 면에서 차이가 많고 활동 환경도 달라서 소비자 단체소송제도를 그대로 모방하는 것에는 많은 문제점이 있다. 예컨대 개인정보 보호단체 중에는 소비자 보호단체만큼이나 큰 규모의 단체는 존재하지 아니하고, 또 개인정보 보호단체는 소비자 보호단체와 달리 대부분이 시·도에 등록되어 있고 중앙행정기관에는 등록된 단체가 없다. 따라서 현재로서는 개인정보 단체소송을 제기할 수 있는 요건을 구비하고 있는 개인정보 보호단체는 전무하며, 그 결과 개인정보 단체소송제도는 무의미한 것이 되고 있다.

2. 개정방향

조정전치주의를 폐지하여 먼저 집단분쟁조정을 신청해 보고

나서 나중에 단체소송을 제기할 것인지 집단분쟁조정절차를 거치지 않고 곧장 단체소송을 제기할 것인지 여부를 정보주체들이 선택할 수 있도록 해야 한다. 조정전치주의는 소비자 단체소송에서도 도입하고 있지 않다.

개인정보 단체소송이 활성화 되도록 단체소송의 원고적격 요건을 소비자단체 소송보다 완화하여야 한다. 현재 상시 개인정보보호 활동을 하고 있는 등록 비영리 민간단체는 2개 정도(진보네트워크, 함께하는 시민행동)에 불과하며 정회원 규모도 1000명 내외이다. 또한 등록 요건도 중앙행정기관에 등록한 비영리 민간단체로 제한하지 말고 지방자치단체에 등록한 단체로까지 확대하여 현재 활동 중인 개인정보 보호단체들에게도 원고적격의 자격을 부여하여야 할 것이다.

개정안 신·구 대조표

현 행	개 정 안
제51조(단체소송의 대상 등) 다음 각 호의 어느 하나에 해당하는 단체는 개인정보처리자가 제49조에 따른 집단분쟁조정을 거부하거나 집단분쟁조정의 결과를 수락하지 아니한 경우에는	제51조(단체소송의 대상 등) 다음 각 호의 어느 하나에 해당하는 단체는 개인정보처리자가 이 법을 위반하여 정보주체의 권리를 계속 침해하고 있는 경우에는 법원에 권리침해 행위

법원에 권리침해 행위의 금지·중지를 구하는 소송(이하 “단체소송”이라 한다)을 제기할 수 있다.	의 금지·중지를 구하는 소송(이하 “단체소송”이라 한다)을 제기할 수 있다.
1. 「소비자기본법」 제29조에 따라 공정거래위원회에 등록한 소비자단체로서 다음 각 목의 요건을 모두 갖춘 단체	1. 「소비자기본법」 제29조에 따라 공정거래위원회에 등록한 소비자단체로서 다음 각 목의 요건을 모두 갖춘 단체
가. 정관에 따라 상시적으로 정보주체의 권익증진을 주된 목적으로 하는 단체일 것	가. 정관에 따라 상시적으로 정보주체의 권익증진을 주된 목적으로 하는 단체일 것
나. 단체의 정회원수가 1천명 이상일 것	나. 단체의 정회원수가 1천명 이상일 것
다. 「소비자기본법」 제29조에 따른 등록 후 3년이 경과하였을 것	다. 「소비자기본법」 제29조에 따른 등록 후 3년이 경과하였을 것
2. 「비영리민간단체 지원법」 제2조에 따른 비영리민간단체로서 다음 각 목의 요건을 모두 갖춘 단체	2. 「비영리민간단체 지원법」 제2조에 따른 비영리민간단체로서 다음 각 목의 요건을 모두 갖춘 단체
가. 법률상 또는 사실상 동일한 침해를 입은 100명 이상의 정보주체로부터 단체소송의 제기를 요청받을 것	가. 법률상 또는 사실상 동일한 침해를 입은 50명 이상의 정보주체로부터 단체소송의 제기를 요청받을 것
나. 정관에 개인정보 보호	나. 정관에 개인정보 보호

를 단체의 목적으로 명시한 후 최근 3년 이상 이를 위한 활동실적이 있을 것 다. 단체의 상시 구성원수가 5천명 이상일 것 라. 중앙행정기관에 등록되어 있을 것	또는 소비자의 권익증진을 단체의 목적으로 명시한 후 최근 3년 이상 이를 위한 활동실적이 있을 것 다. 단체의 상시 구성원수가 1천명 이상일 것 라. 중앙행정기관 또는 지방자치단체에 등록되어 있을 것

3. 유사 입법례

개인정보침해로 피해를 입은 소비자는 소비자기본법에 의해 소비자분쟁조정을 신청하거나 소비자단체소송을 제기할 수도 있다. 다만, 소비자분쟁조정과 소비자단체소송은 소비자와 사업자 간의 분쟁에 대해서만 적용되기 때문에 정보주체와 공공기관 간의 개인정보피해는 소비자기본법에 의한 구제가 불가능하다.

소비자기본법은 「다음 각 호의 어느 하나에 해당하는 단체는 사업자가 제20조의 규정을 위반하여 소비자의 생명·신체 또는 재산에 대한 권익을 직접적으로 침해하고 그 침해가 계속되는 경우 법원에 소비자권익침해행위의 금지·중지를 구하

는 소송(이하 "단체소송"이라 한다)을 제기할 수 있다.」라고 하여 소비자단체소송의 원고가 될 수 있는 자격을 아래와 같이 세 가지 단체로 구분해서 규정하고 있다.[53]

(1) 공정거래위원회에 등록한 소비자단체로서 다음 각 목의 요건을 모두 갖춘 단체

- 정관에 따라 상시적으로 소비자의 권익증진을 주된 목적으로 하는 단체일 것
- 단체의 정회원수가 1천명 이상일 것
- 등록 후 3년이 경과하였을 것

(2) 공인된 사업자단체

- 「상공회의소법」에 따른 대한상공회의소
- 「중소기업협동조합법」에 따른 중소기업협동조합중앙회
- 전국 단위의 경제단체로서 대통령령이 정하는 단체

(3)「비영리민간단체 지원법」에 따른 비영리민간단체로서 다음 각 목의 요건을 모두 갖춘 단체

53) 소비자기본법 제70조 참조.

- 법률상 또는 사실상 동일한 침해를 입은 50인 이상의 소비자로부터 단체소송의 제기를 요청받을 것
- 정관에 소비자의 권익증진을 단체의 목적으로 명시한 후 최근 3년 이상 이를 위한 활동실적이 있을 것
- 단체의 상시 구성원수가 5천명 이상일 것
- 중앙행정기관에 등록되어 있을 것

법원은 소제기단체가 사업자에게 소비자권익 침해행위를 금지·중지할 것을 서면으로 요청한 후 14일이 경과하였으면 단체소송을 허가해야 한다.[54] 소제기 전에 분쟁조정절차를 거쳐야 할 필요는 없다.

54) 소비자기본법 제74조 참조.

제15절 이행강제금제의 신설 (제75조 신설)

1. 현황 및 문제점

개인정보보호법은 이 법을 위반한 자에 대하여 시정 등의 조치명령제도를 도입하고 있으나, 조치명령 미이행자에 대한 제재조치는 5천만 원 이하의 과태료(제75조 제2항 제13호)로 이행강제력이 낮다.

2. 개정방향

시정명령 등에 대한 이행력을 확보하기 위해서는 실효성이 낮은 과태료 제도를 폐지하고 이행강제금 제도를 도입하는 것이 바람직할 것이다. 다만, 이 경우 시정조치명령 미이행에 대한 과태료 부과 규정(제75조 제2항 제13호)은 이중처분의 우려가 있는 만큼 삭제가 필요하다.

개정안 신·구 대조표

현 행	개 정 안
<신 설>	제76조(이행강제금) ① 행정

	안전부장관등은 이 법을 위반하여 제64조에 따른 조치명령을 받은 후 그 정한 기간 내에 이행을 하지 아니한 자에 대하여 매 1일당 500만원의 범위 안에서 이행강제금을 부과할 수 있다. ② 이행강제금의 부과·납부·징수·환급 등에 관하여 필요한 사항은 대통령령으로 정한다. 다만, 체납된 이행강제금은 국세체납처분의 예에 따라 이를 징수한다. ③ 행정안전부장관등은 제1항 및 제2항의 규정에 의한 이행강제금의 징수 또는 체납처분에 관한 업무를 국세청장에게 위임할 수 있다.
제75조(과태료) ① (생 략) ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만 원 이하의 과태료를	제75조(과태료) ①(현행과 같음) ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만 원 이하의 과태료를

부과한다. 1.~12. (생 략) 13. 제64조제1항에 따른 시정명령에 따르지 아니한 자 ③~④ (생 략)	부과한다. 1.~12. (현행과 같음) <삭 제> ③~④ (현행과 같음)

3. 유사 입법례

이행강제금제도는 크게 두 가지 유형으로 나뉜다. 과징금 또는 과태료와 유사하게 1회 부과할 수 있는 이행강제금의 상한선을 정하는 경우가 있고, 지연 일수에 비례해서 이행강제금을 산정해 부과하도록 하는 경우가 있다. 예컨대 근로기준법은 노동위원회로부터 구제명령을 받은 사용자가 이행 기한까지 구제명령을 이행하지 아니한 경우에는 2천만 원 이하의 이행강제금을 부과하도록 규정하고 있고,[55] 전기통신사업법은 방송통신위원회로부터 시정명령을 받은 후 전기통신사업자가 시정명령에서 정한 기간에 이를 이행하지 아니하는 경우에는 하루당 그가 소유한 주식 매입가액의 1천분의 3 이내로 부과하도록 규정하고 있다.[56]

55) 근로기준법 제33조 참조.
56) 전기통신사업법 제13조 참조.

Ⅳ. 개인정보보호법의 규제 투명화・명확화

제1절 개인정보 수집 제한 원칙의 명확화(제16조)

1. 현황 및 문제점

개인정보보호법은 「개인정보처리자가 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다.」라고 하여 최소수집원칙을 규정하고, 「이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.」라고 규정하고 있다. 또한 최소한의 정보 외의 개인정보 제공에 동의하지 않는다는 이유로 재화 또는 서비스의 제공을 거부할 수 없으며 이를 위반하여 재화 또는 서비스의 제공을 거부한 경우에는 3천마원 이하의 과태료를 부과하도록 되어 있다.[57] 따라서 개인정보보호법상 최소수집원칙은 단순한 선언적 규정이 아니라 강제적인 규정이다.

일반적으로 최소수집원칙은 '옵트아웃'제도에서 의미가 큰 원칙이다. 사전에 정보주체의 동의를 받지 않고 개인정보를 수집・처리하기 개인정보처리자는 목적을 구체화하고 그 목적을

57) 개인정보보호법 제75조 제2항 제2호 참조.

달성하기 위하여 필요한 최소한의 개인정보만 수집해야 한다. 이와 달리 '옵트인' 제도 하에서는 개인정보를 수집·이용할 때 특별한 사유가 있는 경우를 제외하고는 정보주체의 동의를 받아야 하므로 최소수집원칙은 상대적으로 의미가 낮다. 동의를 받아서 사용하는 개인정보에 대해서까지 최소수집원칙을 강요할 경우 계약자유의 원칙 또는 사적 자치의 원칙을 침해할 수 있기 때문이다.

그러나, 개인정보보호법 제16조는 '최소수집원칙'을 정보주체의 동의를 받아서 수집하는 경우로까지 확대하고 있어 현실성을 결여하고 있다. 최소수집원칙을 위반하여 재화 또는 서비스의 제공을 거부한 경우 3천만 원 이하의 과태료에 처하도록 되어 있으나 정보주체의 동의를 받아 수집한 경우에는 이미 당사자 간에 수집하는 개인정보의 항목 또는 범위에 대하여 합의가 있었다고 할 수 있으므로 이를 최소수집원칙 위반으로 다루는 것은 불합리하다.

만약 해당 동의가 정보주체에게 지나치게 불공정하다거나 동의를 부정한 수단이나 방법으로 받았다거나 하는 경우에는 다른 법리에 따라 규제하면 된다.

2. 개정방향

최소수집원칙이 단순한 선언이나 권고가 아니고 강제원칙임

을 명확히 하기 위하여 정보주체의 동의를 받아서 수집·이용하는 개인정보에 대하여는 최소수집원칙의 적용 대상에서 제외한다. 동의에 의한 개인정보 수집·이용은 사적 자치의 원칙이 지배되는 영역이다. 이 경우에는 정보주체의 진의에 따른 자유로운 선택권이 침해받지 않도록 동의 받는 방법을 보다 명확히 하면 된다(제22조).

개정안 신·구 대조표

현 행	개 정 안
제16조(개인정보의 수집 제한) ① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.	제16조(개인정보의 수집 제한) ① 개인정보처리자는 제15조제1항 제2호에서 제6호까지에 해당하는 사유로 정보주체의 동의 없이 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.
② 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집	② 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집

에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.	에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

3. 외국사례

2012년 EU Regulation도 최소수집원칙을 채택하고 있지만, 이 원칙을 위반하였다고 해서 곧장 어떤 제재가 부과되는 것은 아니다.[58] 이에 반하여 일본 개인정보보호법은 「개인정보취급사업자는 미리 본인의 동의를 얻지 않고 전조의 규정에 의하여 특정된 이용목적의 달성에 필요한 범위를 초과하여 개인정보를 취급하여서는 아니 된다.」라고 하여 개인정보취급사업자가 정보주체의 동의 없이 취급하는 개인정보에 대해서는 필요 최소한의 원칙이 적용되지만, 본인의 동의를 얻어서 이루어지는 개인정보 취급에 대하여는 필요 최소한의 원칙을 적용시키고 있지 않다.[59]

58) 2012년 EU Regulation 제3조 참조.
59) 일본 개인정보보호법 제16조제1항 참조.

제2절 국외 제3자 제공시 동의 범위의 명확화 (제17조제3항)

1. 현황 및 문제점

개인정보보호법은 개인정보를 '국외의 제3자에게 제공할 때'에는 정보주체에게 알리고 동의를 받아야 한다고 규정하고 있다. 국외의 제3자에게 개인정보를 제공할 때에는 그 만큼 위험성이 커지기 때문에 정보주체의 주의를 환기·유도하기 위한 것이라고 할 수 있다. 그런데 동조는 국외의 제3자에게 개인정보를 제공할 때에는 정보주체의 동의를 받으라고만 되어 있어 모든 형태의 제3자 제공에 대해서 동의를 받으라는 것인지, 제3자 제공에 대하여 정보주체의 동의가 필요한 경우에만 국외의 제3자에게 제공된다는 사실을 특별히 알리고 동의를 받으라는 것인지가 불분명하다.

개인정보보호법 제17조제1항 및 제18조제2항에 대한 특칙으로써, 정보주체의 동의 없이 개인정보를 제공할 수 있는 경우에도 국외 제3자 제공시에는 정보주체의 동의를 받아야 한다는 것이라면 법률의 규정이나 법령상 의무준수, 공공기관의 소관업무 수행 등을 위해 국외의 제3자에게 제공하는 경우 등에도 국외의 제3자에게 제공할 때에는 정보주체의 동의를 받아야 하게 된다. 이 경우 정보주체의 동의가 없으면 국외 제3자 제공은 일체 불가능하게 되어 법률의 집행도 불가능해 질 수

있다.

2. 개정방향

제17조제1항 및 제18조제2항에 따라 제3자 제공에 대한 동의 의무가 없는 경우에는 국외 제3자 제공에 대해서도 동의 의무가 없는 것으로 하여 해석상의 혼란을 피하고, 국외 제3자 제공에 대하여 동의를 받을 때에는 고지 사항에 제공받을 국가의 이름을 추가하도록 하여 국내 제3자 제공과 국외 제3자 제공 사이의 차이를 명확히 하여야 할 필요가 있다.

국외로 이전되는 개인정보 일반에 대한 보호 장치는 국외 제3자 제공에 대한 동의와는 구분해서 앞장(Ⅲ.1)에서 별도로 검토하였다.

개정안 신·구 대조표

현행	개정안
제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하	제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수

같다)할 수 있다. 1. 정보주체의 동의를 받은 경우 2. 제15조 제1항 제2호·제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우 ② 개인정보처리자는 제1항 제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다. 1. 개인정보를 제공받는 자 2. 개인정보를 제공받는 자의 개인정보 이용 목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용	있다. 1. 정보주체의 동의를 받은 경우 2. 제15조 제1항 제2호·제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우 ② 개인정보처리자는 제1항 제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다. 1. 개인정보를 제공받는 자 2. 개인정보를 제공받는 자의 개인정보 이용 목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.	③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공하기 위하여 정보주체의 동의를 받을 때에는 미리 제2항 각 호의 사항 외에 제공받는 국가의 이름을 알려야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

3. 외국사례

국외 제3자 제공에 대하여 정보주체에게 그 사실을 별도로 알리고 동의를 받도록 하고 있는 나라는 우리나라를 제외하고는 발견되지 않는다. 다만, 2012년 EU Regulation은 개인정보처리자가 개인정보를 유럽연합 이외의 지역으로 이전하려는 경우에는 해당 국가가 개인정보 이전 적합국가로 고시되어 있거나 개인정보를 이전받고자 하는 수령자가 구속력 있는 계약 또는 사규를 통해 개인정보의 안전한 보호를 보장하여야 한다. 이 경우 개인정보의 국외 이전이란 제3자 제공에 국한되지 않고, 개인정보 처리위탁, 영업의 양도·양수 등도 포함하는 넓은 개념이다.

제3절 동의 없이 처리할 수 있는 개인정보의 명확화(제22조 제2항)

1. 현황 및 문제점

개인정보보호법은 개인정보처리자가 개인정보를 처리하기 위하여 정보주체의 동의를 받을 때에는 정보주체의 “동의 없이 처리할 수 있는 개인정보”와 정보주체의 “동의가 필요한 개인정보”를 구분하도록 요구하고 있다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.

이처럼 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담하지만, 동조는 “동의 없이 처리할 수 있는 개인정보”가 무엇인지에 대해서 명시하고 있지 아니하여 해석상 혼란이 야기되고 있다. 또한 여기서 정보주체의 “동의가 필요한 개인정보”와 동조 제4항에서 규정하고 있는 “선택적으로 동의할 수 있는 사항”이 같은 의미인지 다른 의미인지를 두고 논란이 계속되고 있다.

2. 개정방향

정보주체의 “동의 없이 처리할 수 있는 개인정보”의 의미를

구체적으로 명시하는 것이 바람직하다. 즉 동조의 목적 또는 취지상 “동의 없이 처리할 수 있는 개인정보”란 제15조 제1항 제2호에서 제6호, 제17조 제1항 제2호, 제18조 제2항 제2호에서 제9호, 제23조 제2호, 제24조 제1항 제2호를 의미하는 것으로 해석하는 것이 타당하므로 이를 법률에 명시하여야 할 것이다.

또한 제15조 제1항 제2호에서 제6호, 제17조 제1항 제2호, 제18조 제2항 제2호에서 제9호, 제23조 제2호, 제24조 제1항 제2호에 의해서 개인정보를 처리한다고 하더라도 정보주체의 동의 없이 처리할 수 있는 개인정보는 필요 최소한의 정보에 한정되므로 “동의 없이 처리할 수 있는 개인정보 = 필요 최소한의 개인정보”의 등식이 성립되도록 하여야 한다.

개정안 신·구 대조표

현 행	개 정 안
제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제5항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각	제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제5항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각

각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다.	각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다.
② 개인정보처리자는 제15조제1항 제1호, 제17조제1항 제1호, 제23조제1호 및 제24조제1항 제1호에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체와의 계약 체결 등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.	② 개인정보처리자는 제15조제1항 제1호, 제17조제1항 제1호, 제23조제1호 및 제24조제1항 제1호에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 제15조제1항 제2호에서 제6호, 제17조제1항 제2호, 제18조제2항 제2호에서 제9호, 제23조제2호, 제24조제1항 제2호에 따라 정보주체의 동의 없이 처리할 수 있는 최소한의 개인정보와 정보주체의 동의가 필요한 개인정보를 명확하게 구분하여야 한다. 이 경우 동의 없이 처리할 수 있는 최소한의 개인정보라는 입증책임은 개인정보처리자가 부담한다.
③ 개인정보처리자는 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하	③ 개인정보처리자는 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하

기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.	기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.
④ 개인정보처리자는 정보주체가 제2항에 따라 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나 제3항 및 제18조제2항 제1호에 따른 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.	④ 개인정보처리자는 정보주체가 제2항에 따라 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나 제3항 및 제18조제2항 제1호에 따른 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.
⑤ 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.	⑤ 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.
⑥ 제1항부터 제5항까지에	⑥ 제1항부터 제5항까지에

서 규정한 사항 외에 정보주체의 동의를 받는 세부적인 방법 및 제5항에 따른 최소한의 정보의 내용에 관하여 필요한 사항은 개인정보의 수집매체 등을 고려하여 대통령령으로 정한다.	서 규정한 사항 외에 정보주체의 동의를 받는 세부적인 방법 및 제5항에 따른 최소한의 정보의 내용에 관하여 필요한 사항은 개인정보의 수집매체 등을 고려하여 대통령령으로 정한다.

3. 유사 입법례

개인정보를 처리하기 위하여 정보주체의 동의를 받을 때 정보주체의 “동의 없이 처리할 수 있는 개인정보”와 정보주체의 “동의가 필요한 개인정보”를 구분하도록 요구하고 있는 입법례는 찾기 어렵다. 동조의 입법 취지는 “동의” 원칙이 남용되고 있는 우리나라만의 독특한 환경에서 정보주체가 거래를 위해서 “불가결한 정보” 또는 “필요 최소한의 정보”라는 이름으로 동의를 강요받지 않게 하기 위한 것이다.

다시 말해 그동안 많은 개인정보처리자들이 개인정보처리에 대한 정보주체의 동의를 받을 때 정보주체가 동의 여부를 선택할 수 있는 사항임에도 불구하고 이를 필수제공정보로 구분하여 사실상 동의를 강요해 왔기 때문에 “동의 없이 처리할

수 있는 개인정보”와 “동의가 필요한 개인정보”를 구분하여 “동의가 필요한 개인정보”에 대하여는 철저하게 정보주체의 선택권을 보장함으로써 동의를 강요하는 관행을 개선·근절하기 위한 것이다.

우리나라 개인정보보호법과 취지는 좀 다르지만, 유럽연합 개인정보보호법안도 정보주체가 “특정한 목적”을 위해 자신의 개인정보가 처리되는 것에 대해 동의했다는 것에 대한 입증책임을 개인정보처리자가 부담하도록 하고 있고, 개인정보처리에 대한 정보주체의 동의가 다른 문제와 관련된 서면진술에 포함되는 경우에는 다른 문제와 구별될 수 있도록 동의 요건이 제시되어야 한다고 규정하고 있다.[60]

제4절 개인정보 처리에 대한 동의방법 유연화(제22조제7항 등 신설)

1. 현황 및 문제점

거래의 행태나 내용에 따라 또는 개인정보를 수집하는 매체, 방법, 시기 등에 따라 개인정보처리자가 정보주체의 동의를 받

60) 2012년 EU Regulation 제7조 참조.

는 방법은 매우 다양할 수 있다. 그러나 현행 개인정보보호법은 동의방법을 매우 획일적·제한적으로 규정하고 있어 현실과 괴리감이 크고, 동의를 형식화 또는 요식화하고 있다는 비판을 받고 있다.

예컨대, 최근 스마트폰의 확산으로 소형 모바일 단말기의 보급·이용이 확대되고 있으나, 모바일 기기는 공간적·시간적 제약으로 인해 정보주체에게 모든 고지사항을 충분히 전달하기 곤란하다. 이처럼 동의를 받는 매체인 단말기의 특성을 고려하지 않게 되면 온라인 서비스 이용 시 고지사항이 너무 많아 고지를 할 수 없거나 너무 작은 글씨로 고지하게 되어 고지내용을 확인하는 것이 곤란해진다. 이 경우 정보주체에게 인터넷 주소 등을 알려주어 동의사항을 확인하게 한 후 다시 전화로 그 동의 사항에 대한 동의의 의사표시를 확인하게 하거나 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법이 허용되고는 있지만 정보주체 중에 그런 불편을 감수하고자 하는 사람은 많지 않을 것이다.[61]

또 개인정보를 제공받을 제3자의 수가 많은 경우에도 제공받을 자를 일일이 알리고 동의를 받아야 한다면 개인정보처리자와 정보주체 모두에게 불필요하게 시간과 비용만 낭비하게 되

61) 개인정보보호법 시행령 제17조 참조.

는 결과를 초래할 수 있다. 예컨대 개인정보를 제공받게 될 300명의 수령인의 이름을 모두 현장에서 구분 없이 알려주고 동의를 받는 것보다는, 동의를 받을 때에는 ○○은행 등 100개 은행, ○○병원 등 100개 병원, ○○쇼핑몰 등 100개 쇼핑몰 등으로 알리고 동의를 받고 구체적인 명단은 별도로 고지하게 하거나 공개하게 하는 것이 정보주체의 권리 보호에 더 부합할 수 있다.

2. 개정방향

현재의 획일적이고 제한적인 동의 방법을 좀 더 유연화해서 개인정보의 수집매체, 업종특성, 정보주체의 수 등을 고려해서 대통령령으로 보다 현실에 맞게 규정할 수 있게 하고, 개인정보 수집 매체의 특성상 공간적·시간적 제약으로 인해 동의 내용을 전부 표시·설명하기 어려운 경우에는 이용자에게 동의 내용을 확인할 수 있는 방법(인터넷주소·수신자부담 ARS 전화번호 등)을 안내하고 동의를 얻을 수 있도록 예외를 허용한다거나 주요 사항에 대해서만 안내하고 구체적인 내용은 별도로 고지 또는 공개할 수 있게 하는 방안을 강구하여야 할 것이다.

개정안 신·구 대조표

현 행	개 정 안
제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제5항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다. ② 개인정보처리자는 제15조제1항 제1호, 제17조제1항 제1호, 제23조제1호 및 제24조제1항 제1호에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체와의 계약 체결 등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다. 이	제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제5항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다. ② 개인정보처리자는 제15조제1항 제1호, 제17조제1항 제1호, 제23조제1호 및 제24조제1항 제1호에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체와의 계약 체결 등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다. 이

경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.	경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.
③ 개인정보처리자는 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.	③ 개인정보처리자는 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.
④ 개인정보처리자는 정보주체가 제2항에 따라 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나 제3항 및 제18조제2항 제1호에 따른 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.	④ 개인정보처리자는 정보주체가 제2항에 따라 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나 제3항 및 제18조제2항 제1호에 따른 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.
⑤ 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인	⑤ 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인

의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.	의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.
<신 설>	⑥ 개인정보처리자는 제15조제1항 제1호, 제17조제1항 제1호, 제23조제1호 및 제24조제1항 제1호에 따라 개인정보의 처리에 대한 동의를 받고자 하는 경우에는 대통령령이 정하는 바에 따라 개인정보의 수집매체, 업종특성, 정보주체의 수 등을 고려하여 동의를 받아야 할 사항을 정보주체가 명확하게 인지하고 확인할 수 있는 방법으로 하여야 한다.
<신 설>	⑦ 개인정보처리자는 개인정보 수집매체의 특성상 정보주체에게 알려야 할 내용을 전부 표시하기 어려운 경우에는 정보주체에게 고지 내용을 확인할 수 있는 방법(인터넷주소·수

	신자부담 전화번호 등)을 안내하고 동의를 얻을 수 있다.
⑥ 제1항부터 제5항까지에서 규정한 사항 외에 정보주체의 동의를 받는 세부적인 방법 및 제5항에 따른 최소한의 정보의 내용에 관하여 필요한 사항은 개인정보의 수집매체 등을 고려하여 대통령령으로 정한다.	⑧ 제5항에 따른 최소한의 정보의 내용과 제7항에 따른 고지내용의 안내방법에 관하여 필요한 사항은 개인정보의 수집매체 등을 고려하여 대통령령으로 정한다.

3. 유사 입법례

독일 등 일부 나라에서 개인정보처리에 대한 동의를 받을 때 문서에 의해서 동의를 받도록 요구하는 경우는 있으나,[62] 개인정보처리에 대하여 정보주체의 동의를 받을 때 수집매체 등에 따라 동의방법을 법률로 정하고 있는 나라는 찾기 어렵다. 한편, 정보통신망법 제12조제2항은 「정보통신서비스제공자등은 개인정보 수집 매체의 특성상 동의 내용을 전부 표시하기 어려운 경우 이용자에게 동의 내용을 확인할 수 있는 방법(인터

62) 독일 연방 개인정보보호법 제4a조 참조.

넷주소, 사업장전화번호 등)을 안내하고 동의를 얻을 수 있다.」라고 규정하여 제한적이지만 휴대전화와 같이 동의 매체가 작은 경우에는 이른바 “참조방식”으로 고지하고 동의 받는 것을 허용하고 있다.

제5절 재위탁·재재위탁의 투명화(제26조제1, 2항 및 제30조제1항)

1. 현황 및 문제점

비용절감, 인력관리 등 경영상의 필요와 손쉬운 데이터 이전 기술로 인해 개인정보 처리 업무의 위탁 및 재위탁이 보편화되고 있다. 게다가 수탁자 또는 재수탁자가 보유하고 있는 개인정보를 활용해 자신의 개인정보를 보강하고 업데이트 시키고자 하는 편법적인 목적의 위탁과 재위탁도 행해지고 있다. 이에 따라 위탁자—수탁자—재수탁자—재재수탁자 등의 관계가 무한정 확대되고 있고 그에 따른 유출·오남용의 위험도 더 커지고 있지만 위탁자의 재수탁자 또는 재재수탁자 등에 대한 관리·감독은 잘 이루어지고 있지 않다.

한편, 개인정보보호법은 위탁하는 업무의 내용과 수탁자의 신

원을 공개하도록 하고 있으나 재위탁 또는 재재위탁 등에 대해서는 관련 규정이 없다. 때문에 재위탁, 재재위탁 등을 통해서 개인정보가 여러 단계에 걸쳐 전전유통되고 있으나 정작 정보주체 자신은 그 사실에 대해서 알지 못하는 경우가 많다. 재위탁이나 재재위탁의 경우 수탁자가 책임을 진다고 할 수 있으나 위탁자도 책임을 면하기 어렵다.

2. 개정방향

개인정보처리자가 개인정보처리업무를 위탁할 때에는 위·수탁계약 체결 시 재위탁, 재재위탁의 등의 금지·제한에 관한 사항을 문서로 명확히 하도록 하여 개인정보처리업무의 재위탁 또는 재재위탁 등이 무분별하게 남용되지 않도록 하여야 한다. 만약 개인정보처리자가 재위탁 또는 재재위탁 등을 허용한 경우에는 그 목적, 범위 등을 명확히 하도록 하여 수탁자, 재수탁자, 재재수탁자 등이 자신의 책임과 의무를 명확하게 인지하게 하여야 한다.

아울러 재위탁, 재재위탁 등이 투명하게 이루어지도록 재위탁, 재재위탁 등의 금지·제한이나 허용에 관한 내용을 개인정보처리방침에 알기 쉽게 공개하도록 하여야 한다.

재위탁, 재재위탁의 남용을 방지하기 위하여 개인정보처리자가 재위탁, 재재위탁 등을 허용할 때에는 미리 정보주체의 동

의를 받게 해야 한다거나 수탁자가 개인정보처리업무를 재위탁할 때에는 정보주체에게 고지하고 동의를 받아야 한다는 주장도 있으나 이는 사적 자치를 지나치게 제한할 우려가 있고 위·수탁제도의 취지에도 맞지 아니함으로 바람직스럽지 않다.

개정안 신·구 대조표

현 행	개 정 안
제26조(업무위탁에 따른 개인정보의 처리 제한) ① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다. 1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 2. 개인정보의 기술적·관리적 보호조치에 관한 사항 <신 설>	제26조(업무위탁에 따른 개인정보의 처리 제한) ① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다. 1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 2. 개인정보의 기술적·관리적 보호조치에 관한 사항 3. 재위탁 또는 재재위탁(이하 “재위탁등”이라 한다)의 금지·제한에 관한 사항(재위탁등을 허용한

	경우에는 그 목적, 범위 등을 포함한다)
3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항	4. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항
② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 “위탁자”라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 “수탁자”라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.	② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 “위탁자”라 한다)는 다음 각 호의 모든 사항을 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다. 1. 위탁하는 업무의 내용 2. 개인정보 처리 업무를 위탁받아 처리하는 자(이하 “수탁자”라 한다) 3. 재위탁등의 금지·제한에 관한 사항(재위탁등을 허용한 경우에는 그 목적, 범위 등을 포함한다)
③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하	③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하

는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.	는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.
④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.	④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.
⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.	⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.
⑥ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해	⑥ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해

배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다. ⑦ 수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.	배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다. ⑦ 수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.
제30조(개인정보 처리방침의 수립 및 공개) ① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 “개인정보 처리방침”이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다. 1. 개인정보의 처리 목적 2. 개인정보의 처리 및 보유 기간 3. 개인정보의 제3자 제공	제30조(개인정보 처리방침의 수립 및 공개) ① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 “개인정보 처리방침”이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다. 1. 개인정보의 처리 목적 2. 개인정보의 처리 및 보유 기간 3. 개인정보의 제3자 제공

에 관한 사항(해당되는 경우에만 정한다) 4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다) 5. 정보주체의 권리·의무 및 그 행사방법에 관한 사항 6. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항	에 관한 사항(해당되는 경우에만 정한다) 4. 제26조제2항 각 호의 사항 5. 정보주체의 권리·의무 및 그 행사방법에 관한 사항 6. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항
② 개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.	② 개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.
③ 개인정보 처리방침의 내용과 개인정보처리자와 정보주체 간에 체결한 계약의 내용이 다른 경우에는 정보주체에게 유리한 것을 적용한다.	③ 개인정보 처리방침의 내용과 개인정보처리자와 정보주체 간에 체결한 계약의 내용이 다른 경우에는 정보주체에게 유리한 것을 적용한다.
④ 행정안전부장관은 개인정보 처리방침의 작성지침	④ 행정안전부장관은 개인정보 처리방침의 작성지침

을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.	을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.

3. 외국사례

일본 개인정보보호법은 재수탁 또는 재재수탁 등에 대하여 특별한 규정을 두고 있지 않다. 다만, 개인정보의 위탁 처리와 관련해서는 「개인정보취급사업자는 개인 데이터의 취급의 전부 또는 일부를 위탁하는 경우에는 그 취급이 위탁된 개인 데이터의 안전한 관리가 도모되도록 위탁을 받은 자에 대한 필요하고 적절한 감독을 행하여야 한다.」라고만 규정하고 있다.[63] 이외에 위탁자나 수탁자에 대하여 어떠한 책임이나 의무도 지우고 있지 않다.

유럽연합도 개인정보의 재수탁 또는 재재수탁 등에 대하여는 특별한 규정을 두고 있지는 않지만, 수탁자는 개인정보처리자의 지시를 받지 않은 사항에 대해서 개인정보를 처리하여서는 안 되고, 수탁자는 개인정보처리자의 사전 동의를 얻은 후에만 개인정보처리에 있어서 다른 사람의 협력을 구할 수 있다고

63) 일본 개인정보보호법 제22조 참조.

규정하고 있다. 그러나 2012년 EU Regulation은 수탁자라는 용어를 사용하고 있지는 않다. 수탁자라는 용어 대산에 '프로세서(processor)'라는 개념을 사용하고 있다는 점이 특징이라고 할 수 있다. 즉 동 법안은 정의에서 「'프로세서'란 개인정보취급자를 대신해서 개인정보를 처리하는 자연인, 법인, 공공기관, 정부기관, 기타의 단체를 의미한다.」라고 규정하고 있다.[64] 따라서 '프로세서'라는 단어를 우리나라 말과 정확하게 일치시키기는 어렵지만, 우리나라의 대리인, 수탁자 등이 모두 포함될 수 있는 개념이라고 할 수 있다.

EU법상 프로세서 즉 수탁자 그 자신과 수탁자의 권한 하에서 개인정보를 취급하는 자는 개인정보처리자의 지시를 받지 않은 사항에 대해서 개인정보를 처리하여서는 안 된다.[65] 수탁자의 권한 하에서 개인정보를 처리하는 자에는 수탁자의 임직원 이외에 재수탁자도 포함된다고 볼 수 있을 것이다. 또한 수탁자는 개인정보처리자의 사전 동의를 얻은 후에만 개인정보처리에 있어서 다른 사람의 협력을 구할 수 있다.[66] 재위탁 또는 재재위탁 등을 금지하는 규정이라고 할 수 있다. 즉 수탁자가 개인정보처리업무를 재위탁하기 위해서는 위탁자의 사전 동의가 필요하다. 그 이외에 재수탁 또는 재재수탁 등에 관하여 다른 특별한 규정을 두고 있지는 않다.

---

64) 2012년 EU Regulation 제4조제6항 참조.
65) 2012년 EU Regulation 제27조 참조.
66) 2012년 EU Regulation 제26조제2항(d) 참조.

제6절 위탁자와 수탁자간 책임 명확화 및 수탁자의 책임 제한 (제26조제7항)

1. 현황 및 문제점

개인정보보호법상 수탁자에게는 개인정보처리업무 위탁(제26조)에 관한 규정을 제외하고 개인정보처리자에 관한 모든 권리·의무규정이 그대로 준용된다. 그러나 해당 준용규정의 목적 또는 취지가 수탁자를 개인정보처리자로 보아 해당 조문들을 준용한다는 것인지, 위탁자의 업무를 처리하는 수탁자로서 준용한다는 것인지가 분명하지 않다. 준용 규정이 업무위탁에 따른 개인정보 처리제한에 관한 규정 속에 포함되어 있는 것으로 보아 위탁자의 업무를 처리하는 수탁자로서 관련 조항들을 준용한다고 보는 것이 타당할 것이다. 그런 의미라면 준용의무를 규정하고 있는 제26조제7항은 규정할 필요가 없는 것이고, 오히려 위탁자와 수탁자 간 책임관계만 애매하게 할 뿐이다.

개인정보처리에 대한 모든 책임과 의무는 원칙적으로 개인정보처리자 자신이 부담해야 한다. 수탁자가 법을 준수하지 아니한 것에 대해서는 민사책임, 형사책임, 행정책임이 각각 다르지만 원칙적으로 각자가 책임을 져야 한다. 즉 법 위반으로 발생한 피해에 대한 손해배상책임에 대해서 수탁자는 당연히 불

법행위자로서 책임을 지지만, 위탁자도 역시 사실상 무과실책임에 가까운 사용자책임을 진다. 또, 수탁자가 저지른 불법행위에 대해서는 개인정보보호법 제74조 양벌규정에 따라 수탁자 자신은 물론 수탁자에 대한 관리·감독을 소홀히 한 위탁자도 형사 처분을 받도록 되어 있다. 수탁자는 제74조에서 규정하고 있는 사용인의 범주에 포함된다고 보기 때문이다.[67] 수탁자의 법위반에 따른 행정책임 즉 과태료에 대해서만 수탁자에게는 책임을 물을 수 없고 위탁자에게만 책임을 물을 수 있다.

이와 같이 수탁자가 수탁업무의 처리과정에서 법을 위반한 경우에는 당연히 민사책임과 형사책임을 지게 되어 있으므로 굳이 준용규정을 둘 필요가 없는 것이다. 또한 위탁자도 수탁자의 불법행위에 대해서 책임을 지기 때문에 수탁자를 잘 관리·감독할 수밖에 없다. 그러나 준용 규정을 둠으로써 하나의 책임 또는 의무를 두 사람이 지는 것이 아니라 위탁자와 수탁자가 각각 다른 책임을 지는 결과를 초래하고 있다. 예컨대, 개인정보를 수집·이용·제공할 때 위탁자와 수탁자는 각자가 정보주체에게 동의를 받아야 하고, 정보주체가 열람요구나 삭제요청을 하면 각자가 열람 또는 삭제조치를 해 주어야 하며, 개인정보 처리방침 작성·공개, 개인정보 유출사고 통지·신고,

67) 이창범, 개인정보보호법, 2012, 법문사, 436쪽 참조. 하급심 판례이지만 수원지법(선고 2005고합160 판결)도 택배위수탁계약에서 수탁자를 "법인의 사용인"으로 보고 있다.

기술적·관리적 보호조치 등도 각자가 중복적으로 해야 한다. 현실적으로 불가능한 것을 요구하는 것이다.

2. 개정방향

원칙적으로 준용규정(제16조제7항)을 삭제하는 것이 바람직하다. 수탁자가 수탁업무처리와 구분된 고유의 업무처리를 위하여 개인정보를 처리하는 경우에는 수탁자도 개인정보처리자로서의 모든 책임과 의무를 지며, 수탁자가 위탁받은 업무를 수행하기 위하여 개인정보를 처리하는 경우에는 이미 민·형사 책임을 물을 수 있는 규정이 마련되어 있으므로 별도의 준용규정은 필요하지 않다.

다만, 개인정보 유출사고 발견 시에는 위탁자에게 신속하게 알려야 한다거나, 위탁자와는 별도로 내부관리계획을 수립해야 한다거나, 개인정보보호책임자를 지정해야 한다거나, 위탁자가 이 법에 위반한 사실을 발견한 경우에는 즉시 그 사실을 위탁자에게 통보하고 적절한 조치를 요구해야 한다는 등과 같은 “수탁자 고유”의 의무규정을 신설하는 것은 의미가 있을 것이다.

한편 최근 A사의 개인정보 유출사건과 관련해서 문제가 되었던 암호화를 포함한 수탁자의 기술적·관리적 보호조치 의무불이행과 관련해서는 제26조제1항에서 위·수탁계약서에 ‘개인

정보의 기술적·관리적 보호조치에 관한 사항'을 명기하도록 되어 있으므로 해당 기술적·관리적 보호조치 의무 위반이 위탁자의 책임인지 수탁자의 책임인지 여부를 판단하면 된다.

개정안 신·구 대조표

현 행	개 정 안
(1안) 제26조(업무위탁에 따른 개인정보의 처리 제한) ① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다. 1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 2. 개인정보의 기술적·관리적 보호조치에 관한 사항 3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항 ② 제1항에 따라 개인정보	(1안) 제26조(업무위탁에 따른 개인정보의 처리 제한) ① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다. 1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 2. 개인정보의 기술적·관리적 보호조치에 관한 사항 3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항 ② 제1항에 따라 개인정보

의 처리 업무를 위탁하는 개인정보처리자(이하 “위탁자”라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 “수탁자”라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.	의 처리 업무를 위탁하는 개인정보처리자(이하 “위탁자”라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 “수탁자”라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.
③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.	③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.
④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니	④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니

하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.	하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.
⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.	⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.
⑥ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.	⑥ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.
⑦ 수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.	<삭 제>

(2안)	(2안)
제26조(업무위탁에 따른 개인정보의 처리 제한) ① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다. 1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 2. 개인정보의 기술적·관리적 보호조치에 관한 사항 3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항 ② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 “위탁자”라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 “수탁자”라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있	제26조(업무위탁에 따른 개인정보의 처리 제한) ① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다. 1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 2. 개인정보의 기술적·관리적 보호조치에 관한 사항 3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항 ② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 “위탁자”라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 “수탁자”라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있

도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.	도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.
③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.	③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.
④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.	④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.
<신 설>	⑤ 수탁자는 개인정보가 분실·도난·유출·변조 또는

	훼손되지 아니하도록 제29조에 따른 내부 관리계획을 수립하고, 제1항에 따라 안전성 확보에 필요한 기술적·관리적 보호조치를 하여야 하며, 개인정보가 분실·도난·유출·변조 또는 훼손된 사실을 발견한 경우에는 즉시 그 사실을 위탁자에게 통보하여야 한다.
⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.	⑥ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 되며, 개인정보가 적법하고 안전하게 처리되도록 제31조에 따른 개인정보보호책임자를 지정하여야 한다.
⑥ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해	⑦ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해

배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다. ⑦ 수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.	배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다. ⑧ 수탁자는 위탁자가 이 법에 위반한 사실을 발견한 경우에는 즉시 그 사실을 위탁자에게 통보하고 적절한 조치를 요청해야 한다.

3. 외국사례

일본 개인정보보호법은 개인정보의 위탁처리에 대해서 별다른 규정을 두고 있지 아니하나, 2012년 EU Regulation은 비교적 상세한 규정을 두고 있다. EU법상 개인정보처리자가 다른 사람에게 개인정보처리업무를 위탁하기 위해서는 법에서 요구하는 기술적·관리적 보호조치를 충분히 이행할 수 있고 정보주체의 권리를 보호할 수 있다는 사실을 보장할 수 있는 하고 하는 자를 처리자(processor)를 선정해야 한다.[68]

또한 수탁자는 구속력 있는 계약이나 법률행위에 의해서만

68) 2012년 EU Regulation 제26조제1항 참조.

개인정보를 처리할 수 있으며 그 계약이나 법률행위에는 다음 각 호의 모든 내용이 포함되어 있어야 한다. 이 경우 위탁자와 수탁자는 아래 위탁자의 모든 지시사항과 처리자의 의무를 서면으로 문서화해야 한다.

(a) 수탁자는 개인정보처리자의 지시에 따라서만 일을 처리한다. 특히 개인정보의 이전(transfer)이 금지되는 경우에는 반드시 개인정보처리자의 지시에 따른다.

(b) 수탁자는 비밀준수의무가 부여되어 있거나 법률상 비밀준수의무를 지고 있는 직원만을 고용해야 한다.

(c) 수탁자는 제30조(기술적·관리적 보호조치)에 의해서 요구되는 모든 보호조치를 취해야 한다.

(d) 수탁자는 개인정보처리자의 사전 동의를 얻은 후에만 개인정보처리에 있어서 다른 사람의 협력을 구한다.

(e) 수탁자는 개인정보처리자와의 합의를 통해 정보주체의 권리행사에 필요한 개인정보처리자의 의무 이행을 위한 기술적·관리적인 요건을 정한다.

(f) 수탁자는 개인정보처리자가 제30조에서부터 제34조에 따른 의무규정을 준수하도록 개인정보처리자를 지원한다.

(g) 개인정보처리업무가 끝난 후에는 모든 결과를 개인정보처리자에게 넘겨주고 더 이상 개인정보를 처리하지 않는다.

(h) 본조에서 규정하고 있는 의무의 준수 여부를 감독하는데 필요한 모든 정보를 개인정보처리자와 관계 감독당국에게 제공한다.

수탁자가 만약 위탁자의 지시 없이 개인정보를 처리하는 경우 수탁자는 해당 개인정보처리와 관련하여 위탁자로 간주되며 제24조에서 규정하고 있는 공동 개인정보처리자에 대한 규정(연대책임)이 적용된다.[69]

이외에도 수탁자는 위탁자의 법률상 책임 또는 의무와는 구별되는 다수의 고유책임을 진다. 예컨대, 수탁자는 자신이 행한 모든 개인정보 처리 활동을 문서로 만들어 보관해야 하는 기록 작성의무(제28조), 감독기관의 자료제출 및 현장조사 요구 등에 대한 협력의무(제29조), 적절한 보안 수준을 보증하기 위한 기술적·관리적 조치의무(제30조), 개인정보 침해사고가 발생한 경우 즉시 위탁자에게 통지해야 할 의무(제31조), 위탁자를 "대신한" 개인정보 영향평가 의무(제33조), 위탁자를 "대

69) 2012년 EU Regulation 제26조제4항 참조.

신한” 개인정보 국외이전 승인의무(제34조), 정보보호 담당자의 지정(제35조) 등이 있다.

제7절 영상정보처리기기의 설치・운영 기준 명확화(제25조)

1. 현황 및 문제점

개인정보보호법은 원칙적으로 “공개된 장소”에 영상정보처리기기의 설치·운영을 금지하고 있지만, 예외적으로 범죄의 예방 및 수사를 위하여 필요한 경우, 시설안전 및 화재 예방을 위하여 필요한 경우, 교통단속을 위하여 필요한 경우, 교통정보의 수집·분석 및 제공을 위하여 필요한 경우, 법령에서 구체적으로 허용하고 있는 경우 등에는 “공개된 장소”에 영상정보처리기기의 설치·운영을 허용하고 있다.

그런데 법 제25조제1항에 따라 예외적으로 정보주체의 동의 없이 영상정보처리기기를 설치・운영할 수 있는 ‘공개된 장소’의 개념이 불명확하여 해석상 혼란을 초래하고 있다. 행정안전부에 따르면 도로, 공원, 공장, 항만, 주차장, 놀이터, 지하철역, 백화점, 대형마트, 상가, 놀이공원, 대중교통(버스, 택시), 아파트단지, 대학구내, 공영주차장은 “불특정 다수”가 출입하거나

이용할 수 있도록 허용된 장소이므로 공개된 장소라고 한다. 더불어 관공서의 민원실, 기업건물의 로비 등도 불특정 다수의 출입이 허용된 곳이므로 공개된 장소로 보아야 한다고 한다. 그러나 관공서의 내부 또는 기업사옥의 내부 공간은 출입이 엄격히 통제되고 내부직원이나 허가를 받은 사람만 출입이 허용되므로 '비공개 장소'라고 한다. 이 경우에는 구성원의 동의를 받거나 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우 등에 한하여 제15조에 따라 영상정보처리기기의 설치·운영이 가능하다.[70]

얼핏 명쾌한 것 같지만 실제로는 애매한 경우가 많다. 그렇다면 출입이 통제되는 학교, 학원, 엘리베이터, 사무실, 물류시설, 호텔복도 등은 공개된 장소인가 아닌가? 행정안전부의 해석에 따르면 사옥 내부나 관공서 내부는 비공개 장소이므로 CCTV를 설치하기 위해서는 제15조에 따라 구성원의 동의를 받거나 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우임을 입증해야 한다. 그렇다면 내부 구성원이 아닌 외부 방문객들에 대해서는 어떻게 동의를 받을 것인가? 이와 같은 장소는 출입이 통제되는 공간이라고 하더라도 출입하는 사람이 계속 바뀌므로 정보주체의 동의를 받는다는 것은 현실적으로 불가능하고, 또 단 한명이라도 정보주체가 동의하지 않으면 CCTV를 설치할 수 없게 되어 버려 다중시설에서의 범죄예방,

70) 행정안전부, 개인정보보호법령및지침·고시해설, 2011.12, 161~164쪽

시설보호 등에 어려움이 따르게 된다.

현실적으로 회사, 공장 등과 같은 사업장에서는 CCTV가 광범위하게 설치·운영되고 있으나 합당한 통제장치가 없다. 대다수 사업장에서 근로자에 대한 고지절차나 동의절차 없이 CCTV가 설치·운영 중에 있으며, 근로자를 대표하는 단체나 조합과의 협의절차나 동의절차도 없이 설치·운영하는 경우가 대부분이다. 「근로자참여 및 협력증진에 관한 법률」은 '사업장 내 근로자 감시 설비의 설치'를 노사협의회의 협의 사항으로 규정하고 있으나 CCTV가 근로자 감시 설비인지에 대해서도 논란이 있을 수 있다.

2. 개정방향

출입통제 여부를 기준으로 공개장소와 비공개장소를 판단할 경우 문리해석 상으로는 올바른 해석일 지라도 CCTV를 설치·운영하고 있는 현실과는 괴리가 크다. 허가를 받고 출입하는 공간이라고 하더라도 하루에도 수백에서 수천 명이 들락거리는 곳이 적지 않고(대학 도서관, 입시학원 복도 등), 출입 통제가 없더라도 공개된 장소로 보기 어려운 곳도 없지 않다(공공 휴게실 등). 따라서 출입통제 여부만을 가지고 공개와 비공개를 구분하는 것은 바람직스럽지 못하다.

공개 장소에서의 CCTV 설치를 허용한 이유가 범죄예방 등

에 있고, CCTV 설치·운영에 대하여 동의를 받는다고 해도 그것은 어디까지나 자발적인 의사에 따른 동의가 아니고 강요된 동의이기 때문에 동의 대신 안내판을 설치하게 해서 정보주체의 사생활을 보호하고자 한 것이라고 할 수 있다. 그렇다고 하면 출입통제가 이루어지고 있는 공간이라도 출입자가 많아(즉 특정다수) 사실상 공개된 장소와 같은 곳이라면 굳이 이를 비공개장소를 볼 필요는 없을 것이다.

그러나 현실적으로 공개된 장소에 대한 다양한 해석이 가능하므로 법해석 및 적용상의 혼란을 피하기 위해서는 법의 제정취지와 현실적 필요를 고려하여 입법적으로 해결할 수밖에 없을 것으로 본다. 즉 영상정보처리기기를 설치·운영할 수 있는 공간에 기존의 공개된 장소 이외에 다수의 사람들이 드나들거나 왕래하는 다중시설의 내·외부도 포함시켜야 한다. 다만, 이 경우 근로자들이 생활하는 작업공간이나 생활공간도 정보주체와의 협의나 동의 없이 영상정보처리기기를 설치·운영할 수 있는 공간이 되어 버려 근로자의 사생활 침해 등 기본권 침해의 우려가 크다. 따라서 근로자의 작업장, 기숙사 등에 영상정보처리기기를 설치·운영하고자 하는 경우에는 노동조합 등 근로자를 대표하는 단체와 사전에 협의절차를 거치도록 명문화해야 할 것이다.

개정안 신·구 대조표

현 행	개 정 안
제25조(영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.	제25조(영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소 또는 여러 사람이 드나들거나 왕래하는 시설의 내·외부에 영상정보처리기기를 설치·운영하여서는 아니 된다.
1. 법령에서 구체적으로 허용하고 있는 경우	1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우	2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우	3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우	4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우	5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우
<신 설>	② 근로기준법 제2조제1항

	제2호에 따른 사용자가 제1항에 따라 사업장, 근로자 기숙사 등에 영상정보처리기기를 설치·운영하고자 하는 경우에는 근로자를 대표하고 있는 단체(노동조합이 구성되어 있는 경우에는 해당 노동조합을 말한다)와 미리 충분한 협의를 하여야 한다.
② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.	③ 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.
③ 제1항 각 호에 따라 영	④ 제1항 각 호에 따라 영

상정보처리기기를 설치·운영하려는 공공기관의 장과 제2항 단서에 따라 영상정보처리기기를 설치·운영하려는 자는 공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.	상정보처리기기를 설치·운영하려는 공공기관의 장과 제2항 단서에 따라 영상정보처리기기를 설치·운영하려는 자는 공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.
④ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자(이하 “영상정보처리기기운영자”라 한다)는 정보주체가 쉽게 인식할 수 있도록 대통령령으로 정하는 바에 따라 안내판 설치 등 필요한 조치를 하여야 한다. 다만, 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.	⑤ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자(이하 “영상정보처리기기운영자”라 한다)는 정보주체가 쉽게 인식할 수 있도록 대통령령으로 정하는 바에 따라 안내판 설치 등 필요한 조치를 하여야 한다. 다만, 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.
⑤ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳	⑥ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳

을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.	을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.
⑥ 영상정보처리기기운영자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 제29조에 따라 안전성 확보에 필요한 조치를 하여야 한다.	⑦ 영상정보처리기기운영자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 제29조에 따라 안전성 확보에 필요한 조치를 하여야 한다.
⑦ 영상정보처리기기운영자는 대통령령으로 정하는 바에 따라 영상정보처리기기 운영·관리 방침을 마련하여야 한다. 이 경우 제30조에 따른 개인정보 처리방침을 정하지 아니할 수 있다.	⑧ 영상정보처리기기운영자는 대통령령으로 정하는 바에 따라 영상정보처리기기 운영·관리 방침을 마련하여야 한다. 이 경우 제30조에 따른 개인정보 처리방침을 정하지 아니할 수 있다.
⑧ 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다. 다만, 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 대통령령으로 정하는 절차 및 요건에 따라야 한다.	⑨ 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다. 다만, 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 대통령령으로 정하는 절차 및 요건에 따라야 한다.

3. 외국사례

대부분의 나라에서 CCTV나 비디오감시는 개인정보보호법에 의해서 이루어지고 있다. 즉 CCTV 등 영상정보처리기기를 이용해서 이미지를 촬영하고 기록하는 것을 개인정보처리로 보고 개인정보보호법상의 개인정보처리원칙(8원칙)을 그대로 적용한다. 따라서 법령에 근거가 있거나, 공공기관이 소관업무 수행을 위해서 필요하거나, 계약의 체결 및 이행을 취해서 필요한 경우, 개인정보처리자의 정당한 이익을 위하여 필요한 경우 등에는 CCTV 등의 설치·운영이 가능하다. 즉 우리나라와 같이 개인정보보호법에 영상정보처리기기의 설치·운영에 관한 별도의 조항을 두지 아니하고 개인정보처리에 관한 일반조항을 해결하고 있다

예컨대 유럽연합 회원국 중 비교적 CCTV를 많이 설치·운영하고 있는 영국의 경우 1998년 제정된 「데이터 보호법」(The Data Protection Act 1998)에 의해서 CCTV가 관리되고 있으며, CCTV 설치·운영 과정에서 데이터 보호법을 올바르게 이해하고 준수하는 것을 돕기 위하여 CCTV 설치·운영을 위한 지침(CCTV code of practice, 2008년 개정)을 제정·권고하고 있다.[71] 영국 데이터 보호법에 따르면 CCTV를 설치·운영하고자 하는 자는 개인정보파일을 구축·운영하고자 하는

71) http://www.ico.gov.uk

자와 마찬가지로 영국의 정보보호기구인 ICO(Information Commissioners Office)에 등록을 하여야 한다. 등록을 하지 아니하면 최고 5천 파운드에 해당한 과태료(fine)가 부과된다. 또한, CCTV 모니터링 시스템은 목적에 적합해야 하고, 모니터링 되고 있다는 사실을 알리기 위한 적절한 안내판을 설치해야 한다. 개인정보보호법상의 목적 명확화 원칙과 고지의무와 동일한 개념이다. 또한 CCTV 모니터링 시스템 관리자는 해당 영상정보에 누가 접근하고, 해당 영상정보를 얼마 동안 보관을 하고, 복제된 영상정보의 처리나 관리는 어떻게 할 것인지를 통제하고 있어야 한다. 또, 모니터링 시스템의 무결성을 유지하기 위한 정기적인 점검과 보수는 필수적이다. 이와 같은 개인정보보호법상의 의무를 준수하지 아니하고 수집한 영상정보는 증거로써 효력이 없고, 과태료에 처해질 수 있으며, 심각한 법 위반의 경우에는 징역형에 처해질 수도 있다.[72]

그러나 일반 개인정보보호원칙이 적용된다고 하여도 EU 국가들마다 차이가 존재한다. 독일은 연방제 국가라서 주마다 다른 법률을 가지고 있지만, 일반적으로 공공기관에 대해서는 CCTV 설치를 엄격히 규제하고 있으며 CCTV 설치를 허용하는 경우에도 경찰에 한해서 범죄 예방 등 목적으로만 허용한다. 프랑스에서는 공공기관이든 민간단이든 CCTV를 설치·운영하기 위해서는 신고를 하고 허락을 받아야 한다. 스웨덴도

72) 영국 IOC 공식 홈페이지(http://www.ico.gov.uk/for_the_public/topic_specific_guides/cctv.aspx) 참조.

CCTV를 설치·운영하기 위해서는 일정한 요건을 갖추어 관계당국에 신청을 하고 승인을 받아야 한다. 작업장에 설치할 때에는 근로자의 동의서를 첨부해야 한다. 승인은 CCTV 감시를 통해서 얻고자 하는 이익과 개인의 사생활 이익을 형량하여 전자가 더 우월한 경우에만 내려진다. 그러나 CCTV 설차는 오로지 범죄의 예방과 탐지 목적으로만 이용될 수 있고, 카메라가 고정되어 있어야 하며, 줌(zoom) 기능을 포함하고 있어서는 안 된다.[73]

한편, 호주의 경우에는 대부분의 주가 CCTV를 포함한 감시장비의 설치·활용에 관하여 별도의 개별법을 두고 있다. 주에 따라 명칭은 Workplace Surveillance Act 2005(뉴사우스웨일스), Surveillance Devices Act 2007(Northern Territory, 빅토리아, 웨스튼 오스트리아) 등 매우 다양하다. 또 주 공공기관들에 대해서는 별도로 「공공장소에서 CCTV의 설치·운영에 관한 가이드라인」[74]이 제정·운영되기도 한다. 하지만 이 모든 주 법령과 가이드라인은 기본적으로 연방 프라이버시법(Privacy Act 1988)의 테두리 내에서 그 내용을 좀 더 구체화하기 위해서 제정된 것이다. 때문에 주요 내용도 CCTV를 설

73) CCTV 설치·운영에 관한 좀 더 자세한 내용은 Marianne L. Gras, The Legal Regulation of CCTV in Europe, Surveillance & Society CCTV Special (eds. Norris, McCahill and Wood) 참조.

74) A NSW Government Initiative, NSW Government Policy Statement and Guidelines for the Establishment and Implementation of CCTV in Public Places.

치·운영하는 목적을 알리도록 요구하거나, 공개된 목적 이외로의 사용을 금지하거나, 정보주체로 하여금 CCTV가 모니터링하고 있다는 사실을 알게 하거나, 이해당사자의 의견을 듣도록 요구하고 있다. 다만, 공공기관은 CCTV를 설치할 때에는 설치 지역 내에서 발생한 범죄(crimes)를 확인할 목적으로만 사용할 수 있고, “명백하게” 범죄와 관련이 있지 아니한 사람을 모니터링하거나 추적할 목적으로는 결코 사용되어서는 안된다고 규정하고 있다. 또한 CCTV는 일반적인 정보(general intelligence)를 수집할 목적으로는 사용될 수 없다.

Ⅴ. 개인정보보호법과 글로벌 스탠더드의 조화

제1절 동의 없는 개인정보 제3자 제공사유 확대(제17조제1항)

1. 현황 및 문제점

개인정보보호법은 정보통신망법과 달리 개인정보처리에 대하여 “동의원칙”을 채택하고 있지 않다. 즉, 정보통신망법은 정보통신서비스 제공자가 이용자의 개인정보를 이용하려고 수집하는 경우에는 동의를 받아야 한다고 하여 동의원칙을 채택하고 있지만,[75] 개인정보보호법상 “동의”는 개인정보처리자가 정보주체의 개인정보를 처리할 수 있는 여러 사유 또는 조건 중 하나에 불과하다.[76] 개인정보 중에는 비밀에 해당하여 처음부

---

75) 정보통신망법 제22조(개인정보의 수집·이용 동의 등) ① 정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 경우에도 또한 같다.
1. 개인정보의 수집·이용 목적
2. 수집하는 개인정보의 항목
3. 개인정보의 보유·이용 기간
② 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 제1항에 따른 동의 없이 이용자의 개인정보를 수집·이용할 수 있다.
1. 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우
2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
3. 이 법 또는 다른 법률에 특별한 규정이 있는 경우

76) 제15조(개인정보의 수집・이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목

터 다른 사람의 사용이 금지되거나 제한된 것도 있지만, 일반적으로 개인정보는 사용을 위하여 만들어지거나 생성되거나 부여된 것이므로 개인정보보호법이 동의원칙을 채택하지 않은 것은 지극히 당연하고 옳다.

그러나 개인정보보호법은 개인정보의 수집·이용의 경우와 달리 제3자 제공에 대해서는 매우 엄격한 처리원칙을 채택하여 사실상 동의원칙을 채택하고 있는 것과 별 차이가 없게 하고 있다. 즉 개인정보보호법상 개인정보처리자는 ⅰ) 정보주체와의 계약 체결 및 이행을 위하여 불가피하게 필요한 경우,

---

적의 범위에서 이용할 수 있다.
1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.
② 개인정보처리자는 제1항 제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
1. 개인정보의 수집·이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

ii) 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우 등에도 정보주체의 동의를 받아야 한다.[77]

이와 같이 거래를 위해서는 당연하게 개인정보의 제공 또는 공유가 필요하거나 정보주체가 개인정보의 제공이나 공유를 예상하거나 예상할 수 있는 경우에까지 정보주체의 동의를 받으라고 함으로써 동의원칙이 남용되어 권리보호 장치로써의 의미가 유명무실해 지고, 경제·사회 활동 전반에 걸쳐 심각한 기능장애와 불필요한 비용을 초래하고 있다.

예컨대, 제휴카드 발급, 유학알선, 국제결혼 등을 위해서는 개인정보의 제3자 제공이 필수적이나 현행 개인정보보호법상으로는 이 경우에도 동의를 받아야 한다. 또, 개인정보처리자가 소비자에 대해 가지고 있는 채권추심, 채권양도, 소송제기 등의 경우에도 개인정보를 채권추심자, 채권양수인, 법원·수사기관·변호사 등에게 제공하여야 하는데 정보주체의 동의를 받지 못하면 채권추심, 채권양도, 소송제기 등도 할 수 없다고 하는 극단적인 상황이 발생할 수도 있다.[78]

이처럼 동의원칙이 남용되다 보니 동의 없이 처리할 수 있는 최소한의 개인정보와 정보주체의 자발적인 선택권이 보장되어

77) 개인정보보호법 제17조 참조.
78) 개인정보처리자가 채권추심을 신용정보업자에게 의뢰한 경우에는 신용정보의 이용 및 보호에 관한 법률에 의해서 일정한 예외가 인정된다.

야 할 개인정보의 처리 사이에 경계가 애매해져 정보주체들이 제3자 제공에 대하여 사실상 동의를 강요받고 있는 상황이다.

2. 개정방향

정보주체의 동의 없이 개인정보를 제공할 수 있는 사유를 사회적 상식과 국제적 스탠더드에 맞게 확대해야 한다. 개인정보 제3자 제공이 문제가 되는 것은 주로 개인정보를 영리 목적으로 판매 또는 대여하거나 합당한 사유 없이 개인정보를 당초 수집한 목적 외로 제공하는 것이다. 따라서 이런 경우에 한해서 정보주체의 동의를 받게 하면 동의를 해야 할 사항이 한, 두 가지 내지 두, 세 가지로 매우 간소해져 정보주체가 자신의 선택권 내지 동의권을 확실히 행사할 수 있게 된다.

이와 같은 견지에서 제3자 제공시 정보주체의 동의를 받아야 할 경우를 정보주체가 예상하기 어려운 경우로 한정해야 하며, 정보주체와의 계약 체결 및 이행을 위하여 불가피하게 필요한 경우, 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우 등에는 정보주체의 동의 없이 개인정보를 제3자에게 제공하는 것을 허용하여야 한다.

개정안 신·구 대조표

현행	개정안
제17조(개인정보의 제공)① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다. 1. 정보주체의 동의를 받은 경우 2. 제15조제1항__제2호·제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우 ② 개인정보처리자는 제1항 제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다. 1. 개인정보를 제공받는 자	제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다. 1. 정보주체의 동의를 받은 경우 2. 제15조제1항__제2호에서 제6호까지에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우 ② 개인정보처리자는 제1항 제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다. 1. 개인정보를 제공받는 자 2. 개인정보를 제공받는 자

2. 개인정보를 제공받는 자의 개인정보 이용 목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 ③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.	의 개인정보 이용 목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 ③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

3. 외국사례

유럽연합도 우리나라 개인정보보호법과 마찬가지로 개인정보 처리에 대하여 동의원칙을 채택하고 있지 아니하며, 이와 같은 입법정책을 개인정보 수집·이용 시는 물론 제3자 제공시에까

지 그대로 유지하고 있다. 우리나라 개인정보보호법과 정보통신망법은 앞에서 살펴본 바와 같이 개인정보의 수집·이용과 제3자 제공을 차별적으로 처리하기 위해 양자의 요건을 엄격하게 구분하고 있지만, 유럽연합은 개인정보 수집·이용과 제3자 제공을 차별하지 아니하고 동일한 기준을 적용하고 있다. 따라서 우리나라와 달리 정보주체와의 계약 체결 및 이행을 위하여 필요한 경우나 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우에도 정보주체의 동의 없이 개인정보를 제3자에게 제공할 수 있다.

일본은 개인정보처리에 대하여 옵트아웃(OPT-OUT) 제도를 도입하고 있다. 따라서 제3자 제공에 대해서도 제공사실, 제공목적 등을 알리기만 하면 되고 동의를 받을 필요는 없다. 또한 특정한 자와의 사이에 개인정보를 공동으로 이용한다는 사실을 미리 밝힌 경우(계열사, 협력회사 등)에는 정보주체의 동의가 없더라도 공동이용이 가능하다. 하지만, 사전에 제3자 제공 사실을 정보주체에게 통지하거나 용이하게 알 수 있는 상태로 알리지 아니한 경우에는 미리 정보주체의 동의를 받거나 동의 예외사유에 해당해야만 제3자 제공이 가능하다. 따라서 일본의 경우에는 개인정보를 수집할 때 계약 체결 및 이행을 위해서 이용·제공한다거나 개인정보처리자의 정당한 이익을 위해서 이용·제공한다는 사실을 미리 밝히기만 하면 되며 동의를 받을 필요는 없다.

개인정보 제3자 제공기준 비교

2012년 EU Regulation 제6조	일본 개인정보보호법 제23조
제6조(처리의 적법성) 1. 개인정보 처리는 다음 중 하나 이상에 해당하는 경우에만 적법하다. (a) 정보주체가 하나 이상의 구체적인 목적을 위해 자신의 개인정보 처리에 동의를 하는 경우; (b) 정보주체가 계약 당사자인 계약의 이행을 위해 또는 계약 체결 전 정보주체의 요청에 따라 조치를 취하기 위해 개인정보 처리가 필요한 경우; (c) 개인정보처리자가 의무의 주체인 법률상의 의무를 준수하는데 필요한 경우; (d) 정보주체의 중요한 이익을 보호하기 위해 필요한 경우; (e) 공익을 위해 필요하거나 또는 개인정보처리자에게 부여된 공적인 권한의 행사를 위해 필요한 경우;	제23조(제3자 제공의 제한) ①개인정보취급사업자는 다음에 게재하는 경우를 제외하고는 미리 본인의 동의를 얻지 않고 개인 데이터를 제3자에게 제공할 수 없다. 1. 법령에 근거한 경우 2. 사람의 생명, 신체 또는 재산의 보호를 위하여 필요한 경우로서 본인의 동의를 얻는 것이 곤란한 때 3. 공중위생의 향상 또는 아동의 건전한 육성의 추진을 위하여 특히 필요한 경우로서 본인의 동의를 얻는 것이 곤란한 때 4. 국가기관, 지방공공단체 또는 그 위탁을 받은 자가 법령에서 정한 사무를 수행하는 것에 대해서 협력할 필요가 있는 경우로서, 본인의 동의를 얻는 것에 의해 당해 사무의 수행에 지장을 줄 우려가 있는 때

(f) 개인정보처리자가 추구하는 정당한 이익의 목적에 부합하는 경우(정보주체 특히 아동의 이익 또는 기본권리 및 자유가 개인정보처리자의 이익보다 우월한 경우는 제외). 그러나 공공기관이 업무를 수행하는 과정에서 처리하는 개인정보에 대해서는 이 항이 적용되지 아니한다. 2. 역사, 통계, 과학연구를 위해 필요한 개인정보의 처리는 제83조에서 규정한 조건과 보호조치에 따르는 한 적법하다.	② 개인정보취급사업자는 제3자에게 제공된 개인 데이터에 관하여 다음 각 호에 게재된 사항에 관하여 미리 본인에게 통지 또는 본인이 용이하게 알 수 있는 상태로 하고 있는 경우에는 전항의 규정에 상관없이 당해 개인데이터를 제3자에 제공할 수 있다. 1. 제3자로의 제공을 이용목적으로 하는 것 2. 제3자에게 제공된 개인데이터의 항목 3. 제3자로의 제공 수단 또는 방법 4. 본인의 요구에 따라 당해 본인이 식별되는 개인데이터의 제3자로의 제공을 정지하는 것 ③~④ (생 략)

제2절 개인정보의 목적 외 이용・제공 사유 축소(제18조)

1. 현황 및 문제점

개인정보보호법은 제15조에서 개인정보의 수집・이용에 관한 기준을 정하고, 제17조에서 개인정보의 제3자 제공(공유를 포함한다)에 관한 기준을 정하고 있다. 그리고 개인정보를 목적 외로 이용하거나 제3자에게 제공하고자 하는 경우에는 이용・제공의 목적, 이용・제공되는 개인정보의 항목, 이용・제공되는 개인정보의 보존기간, 개인정보를 제공받는 수령인 등에 하나라도 변경이 있는 경우에는 정보주체에게 그 사실을 알리고 동의를 받도록 되어 있다.[79]

동시에 제18조는 개인정보의 이용・제공 제한이라는 제목으로 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다고 규정하고, 그럼에도 불구하고 정보주체의 “별도” 동의가 있는 경우, 다른 법률에 특별한 규정이 있는 경우, 정보주체 및 제3자의 생명・신체. 재산 보호를 위해 필요한 경우, 통계작성・학술연구 등을 위해 필요한 경우, 목적 외 이용・제공을 하지 아니하면 공공기관이 소관업무를 수행할 수 없는 경우, 국제협정 이행을 위해 필요한 경우, 수사・소제기 및 유지를 위해 필요한 경우,

79) 개인정보보호법 제15조 제2항 후문 및 제17조 제2항 후문 참조.

재판업무 수행을 위해 필요한 경우, 형·감호·보호처분집행을 위해 필요한 경우[80]에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다고 규정하고 있다.

그러나 이는 사실상 불필요한 조항으로 개인정보처리자와 이용자 모두에게 혼란만 야기하고 있다. 제18조 제2항 제1호는 제15조 제2항 후문과 제17조 제2항 후문에서 규정하고 있는 변경 동의와 같은 것이고, 제18조 제2항 제2호부터 제9호까지는 제15조 제1항 제2호에서 제6호 및 제17조 제1항 제1호에서 규정하고 있는 것과 마찬가지로 "동의" 이외에 개인정보를 적법하게 이용 또는 제공할 수 있는 사유에 해당한다. 즉 제15조 제1항 제2호에서 제6호 및 제17조 제1항 제1호에서 규정하고

80) 1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

있는 사항들과 제18조 제2항 제2호에서 제9호의 사항들은 정보주체의 동의를 받지 않고 개인정보를 이용 또는 제공한다는 측면에서 모두 개인정보의 목적 외 이용 또는 제공이라고 할 수 있다.

그럼에도 불구하고 제18조 제2항에서 개인정보의 목적 외 이용·제공 사유를 다시 규정함으로써 제15조 및 제17조와 차이가 생기고 혼란이 야기되고 있다.

2. 개정방향

제18조제2항 제1호는 변경 동의에 해당하고, 제18조제2항 제2호에서 제9호는 모두 개인정보를 동의 없이 목적 외로 이용 또는 제공할 수 있는 사유들로써 이미 제15조제1항과 제17조제1항에서 규정하고 있는 사항들과 같은 성격의 것이다. 다만, 제18조제2항에는 제15조제1항과 제17조제1항에서 규정하고 있지 아니한 다음 각 호의 사유가 일부 추가되어 있을 뿐이다.

4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우

5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게

제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우

6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우

7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우

8. 법원의 재판업무 수행을 위하여 필요한 경우

9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

제4항을 제외하고 나머지는 모두 공공기관에만 적용된다. 따라서 제18조는 공공기관을 위한 특례조항이라고 할 수 있다. 그러나 제6조에서 제9호까지는 해당 호가 없다고 하더라도 이미 다른 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 또는 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우에 해당하여 개인정보를 수집·이용 또는 제공하는데 아무런 제약이나 장애가 없다. 따라서 불필요한 것이다.

제5호는 우리나라의 개인정보보호제도가 아직 정착되어 있지 아니하고, 각각의 개별법들이 개인정보보호를 충분히 예상해서 제정된 법률이 아니므로 개인정보보호법을 그대로 적용할 경

우 공공기관의 업무수행에 장애가 발생하는 경우가 있을 수 있으므로 한시적으로 동호를 유지하는 것은 상당한 의미가 있다고 할 수 있다.

마지막으로 제4호의 통계작성 및 학술연구 등의 목적은 사실상 제15조와 제17조에서 목적 외 이용 또는 제공 사유로 반영되어 있어야 하는 사항이다. 대다수 국가들이 통계작성 및 학술연구 등의 목적에 대하여는 일정한 안전조치를 전제로 하여 정보주체의 동의 없는 이용 또는 제공을 허용하고 있다. 그러나 개인정보보호법은 목적 외 이용·제공 사유의 하나로 “통계작성 및 학술연구 등”을 인정하면서 “특정 개인을 알아볼 수 없는 형태로 개인정보를 제공”하라고 규정하고 있어 사실상 동의를 받지 않고는 개인정보를 통계작성 및 학술연구 등의 목적으로 이용할 수 없게 하고 있다.[81]

따라서 제18조제2항 제6호에서 제9호는 이를 삭제하고, 제4호는 그 의미를 살려 제58조(적용의 일부 제외)로 이전해서 별도로 규정하고, 제5호만 존치하는 것으로 개정하는 것이 바람직할 것이다.

81) 해당 데이터가 “특정 개인을 알아볼 수 없는 형태”라면 이미 개인정보보호법상의 개인정보가 아니므로 굳이 법에서 동의의 예외사유로 규정할 필요조차 없다.

개정안 신·구 대조표

현 행	개 정 안
제18조(개인정보의 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.	제18조(개인정보의 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다. 다만, 공공기관이 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우에는 그러하지 아니한다.
② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를	<삭 제>

목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다. 1. 정보주체로부터 별도의 동의를 받은 경우 2. 다른 법률에 특별한 규정이 있는 경우 3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우 5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수	

없는 경우로서 보호위원회의 심의·의결을 거친 경우 6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우 7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우 8. 법원의 재판업무 수행을 위하여 필요한 경우 9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우	
③ 개인정보처리자는 제2항 제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다. 1. 개인정보를 제공받는 자 2. 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다) 3. 이용 또는 제공하는 개인정보의 항목	<삭 제>

4. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다) 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용	
④ 공공기관은 제2항 제2호부터 제6호까지, 제8호 및 제9호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 행정안전부령으로 정하는 바에 따라 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.	<삭 제>
⑤ 개인정보처리자는 제2항 각 호의 어느 하나의 경우에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대	⑤ 공공기관은 제1항 단서에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정

하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.	보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.

3. 외국사례

유럽연합, 일본, 미국 등에서는 개인정보의 목적 외 이용·제공에 관한 별도의 규정을 두고 있지 않다. 유럽연합 개인정보보호법안은 제6조제1항에서 개인정보처리의 적법성 원칙 내지 기준을 제시하고 있으며, 제4항에서는 개인정보를 추가로 처리하는 목적이 개인정보를 수집할 당시의 목적과 다른 경우(the purpose of further processing is not compatible with the one for which the personal data have been collected)에는 제1항 각 호의 사유 중 하나에 해당하여야 한다고 규정하고 있다. 여기서 개인정보를 추가로 처리하는 목적(the purpose of further processing)이란 개인정보의 목적 외 이용·제공과 같은 의미라고 볼 수 있다. 다만, "개인정보처리자가 추구하는 정당한 이익의 목적에 부합하는 경우"는 목적 외 이용·제공

사유에 해당하지 않는다. 제18조 제1항에서 개인정보처리자가 추구하는 정당한 이익을 위하여 필요한 경우에 동의 없이 개인정보를 수집하여 이용 또는 제공할 수 있도록 폭넓은 예외를 허용하고 있는데, 여기에 다시 예외를 인정할 경우 남용의 우려가 있기 때문으로 판단된다.

일본은 옵트아웃(OPT-OUT) 제도를 도입하고 있기 때문에 이용 또는 제공 목적을 구체화해서 고지하기만 하면 언제든지 개인정보를 수집하여 이용·제공할 수 있다. 그러나 이미 목적을 정해서 수집한 개인정보를 목적 외로 이용 또는 제공하기 위해서는 미리 정보주체의 동의를 받거나(이른바 변경 동의라고 할 수 있다), 사람의 생명, 신체 또는 재산의 보호를 위해 필요한 경우, 공중위생의 향상 또는 아동의 건전한 육성의 추진을 위하여 특히 필요한 경우, 국가기관·지방공공단체 또는 그 위탁을 받은 자가 법령에서 정한 사무를 수행하는 것에 대해서 협력할 필요가 있는 경우에 한해서만 목적 외 이용 또는 제공이 가능하다.

2012년 EU Regulation 제6조	일본 개인정보보호법 제23조
제6조(처리의 적법성) 1. 개인정보 처리는 다음 중 하나 이상에 해당하는 경우에만 적법하다.	제23조(제3자 제공의 제한) ①개인정보취급사업자는 다음에 게재하는 경우를 제외하고는 미리 본인의

(a) 정보주체가 하나 이상의 구체적인 목적을 위해 자신의 개인정보 처리에 동의를 하는 경우; (b) 정보주체가 계약 당사자인 계약의 이행을 위해 또는 계약 체결 전 정보주체의 요청에 따라 조치를 취하기 위해 개인정보 처리가 필요한 경우; (c) 개인정보처리자가 의무의 주체인 법률상의 의무를 준수하는데 필요한 경우; (d) 정보주체의 중요한 이익을 보호하기 위해 필요한 경우; (e) 공익을 위해 필요하거나 또는 개인정보처리자에게 부여된 공적인 권한의 행사를 위해 필요한 경우; (f) 개인정보처리자가 추구하는 정당한 이익의 목적에 부합하는 경우(정보주체 특히 아동의 이익 또는 기본권리 및 자유가 개인정보처리자의 이익보다 우월한 경우는 제외). 그러나	동의를 얻지 않고 개인 데이터를 제3자에게 제공할 수 없다. 1. 법령에 근거한 경우 2. 사람의 생명, 신체 또는 재산의 보호를 위하여 필요한 경우로서 본인의 동의를 얻는 것이 곤란한 때 3. 공중위생의 향상 또는 아동의 건전한 육성의 추진을 위하여 특히 필요한 경우로서 본인의 동의를 얻는 것이 곤란한 때 4. 국가기관, 지방공공단체 또는 그 위탁을 받은 자가 법령에서 정한 사무를 수행하는 것에 대해서 협력할 필요가 있는 경우로서, 본인의 동의를 얻는 것에 의해 당해 사무의 수행에 지장을 줄 우려가 있는 때

공공기관이 업무를 수행하는 과정에서 처리하는 개인정보에 대해서는 이 항이 적용되지 아니한다. 2. 역사, 통계, 과학연구를 위해 필요한 개인정보의 처리는 제83조에서 규정한 조건과 보호조치에 따르는 한 적법하다. 3. (생 략) 4. 개인정보를 추가로 처리하는 목적이 개인정보가 수집된 목적과 일치하지 않는 경우 제1항의 (a)—(e)에서 언급된 근거 중 최소한 하나 이상에 해당되는 법률적 근거를 갖추고 있는 경우에만 개인정보를 처리할 수 있다. 특히 이는 계약 조건이 변경되는 경우 반드시 적용되어야 한다.	

제3절 불특정 다수에 대한 개인정보 공개 등 기준 마련(제18조의2 신설)

1. 현황 및 문제점

개인정보보호법은 개인정보의 수집·이용, 제공(공유를 포함한다), 위탁, 보관·파기, 영업양도 등에 대해서만 규정하고 불특정 다수에 대한 개인정보의 공개·공유에 대해서는 규정하고 있지 않다. 즉 현행 개인정보보호법은 제17조제2항과 제18조제2항에서 개인정보의 제공 및 공유에 대한 처리기준을 규정하고 있기는 하지만, 이는 “특정된 제3자”에 대한 개인정보의 제공이나 공유를 전제로 하는 것일 뿐, 불특정 제3자에 대한 개인정보의 제공, 공유, 공개에 대해서는 규정이 없다.

이로 인해 불특정다수에 대한 개인정보의 공유와 공개를 전제로 하고 있는 서비스(SNS 등)에 있어서 어떤 절차와 방법에 따라 개인정보를 수집·공개 등을 해야 하는지가 불분명하다. 만약 불특정 다수에 대한 개인정보의 공개 등을 제17조제2항 및 제18조제2항에서 규정하고 있는 제3자 제공 또는 공유의 한 형태로 본다면 카카오톡, 미투데이, 페이스북, 트위터 등 현행 사회관계망서비스(SNS)는 모두 불법이 된다. 이들 서비스는 사회관계망서비스의 고유 특성상 개인정보를 제공받는 자를 특정할 수 없어 제공받는 자를 일반공개, 친구공개 등 카

테고리로만 고지되어 있기 때문이다.

이로 인해 불특정 제3자에 대한 개인정보의 제공, 공유, 공개가 개인정보보호법상 사각지대로 남아 있다. 현행 개인정보보호법의 적용 시 사회관계망서비스의 전면적인 제공 중단 등 문제가 발생한다고 해서 이와 같은 불특정 다수에 대한 개인정보 공개 등을 개인정보보호법의 보호 대상이 아니라고 하여 방치해 둘 수도 없다. 이를 방치해 둘 경우 수천만 명에 이르는 국내 정보주체들의 권리를 보호할 길이 없기 때문이다.

2. 개정방향

개인정보처리자가 개인정보를 수집할 때 미리 개인정보의 제공・공유・공개 등의 목적, 범위, 항목 등을 설정해 두는 행위를 금지하여야 한다(privacy by default). 개인정보를 공개 또는 공유로 디폴트해 놓을 경우 설령 정보주체에게 디폴트를 해제하거나 조정할 수 있는 방법을 제공하더라도 대다수 정보주체들이 디폴트 해제 및 조정 방법을 알기 어렵기 때문에 정보주체의 자유로운 의사에 반하여 개인정보가 공개될 수 있다. 따라서 정보주체가 필요에 따라 스스로 공개 등의 목적, 공개 등의 상대방, 공개 등을 할 개인정보의 항목 등을 선택할 수 있게 하여야 하고, 또한 정보주체가 원하는 경우에는 언제든지 손쉽게 공개 등의 전부 또는 일부를 철회하거나 취소할 수 있

도록 하여야 한다.

다만, 공공의 이익 등을 위해 불가피하게 정보주체의 개인정보를 공개 등을 해야 할 필요가 있으므로 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우에는 예외적으로 불특정 제3자에 대한 개인정보 공개 등을 허용하여야 한다. 예컨대 중대범죄자에 대한 공개수배, 아동성범죄 등의 인터넷공개, 관계법령 위반 사업자의 명단공개(개인사업자), 공무원의 이름·직무 공개 등은 관련 법령에 따라 허용하여야 한다.

개정안 신·구 대조표

현 행	개 정 안
<신 설>	제18조의2(개인정보의 공개 등) ① 개인정보처리자는 다음 각 호의 하나에 해당하는 경우에는 특정되어 있지 아니한 제3자에게 개인정보를 제공·공개하거나 공유(이하 “공개 등”이라 한다)할 수 있다. 1. 정보주체가 스스로 자신의 개인정보를 공개 등을

	하거나 선택한 경우 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우 ② 개인정보처리자는 개인정보를 수집할 때 미리 공개 등으로 설정해 두어서는 안 되며 정보주체가 스스로 공개 등의 상대방, 공개 등을 할 개인정보의 항목 또는 범위를 선택할 수 있게 하여야 하고 언제든지 손쉽게 공개 등을 전부 또는 일부 철회할 수 있게 하여야 한다.

3. 외국사례

유럽연합과 일본, 미국 등은 개인정보의 제공, 공유, 공개 등에 있어서 상대방의 이름을 특정할 필요가 없다. 즉 불특정 다

수에 대한 개인정보 공개 등에 있어서도 개인정보보호원칙이 그대로 적용된다. 예컨대 유럽연합 개인정보보호법안은 개인정보 제3자 제공에 대한 고지·동의를 받을 때 제공받게 될 수령자의 이름을 알리고 동의를 받는 것은 물론이고, 제공받을 자의 범주(categories)만을 정해서 알리고 동의를 받는 것도 가능하다. 한편 2012년 EU Regulation은 개인정보처리자는 개인정보처리시스템을 구축할 때 처음부터 "각각의" 구체적인 처리목적에 필요한 개인정보만을 처리하도록 구축하여야 하고, 처리목적에 필요한 최소한의 범위를 벗어난 개인정보가 수집, 보관되지 않도록 시스템적으로 보장할 것을 요구하고 있고, 더 나아가 불특정 다수가 개인정보처리시스템에 접근할 수 있도록 설정해서는 안 된다고 규정하고 있다.[82]

한편, 일본 개인정보보호법은 제3자 제공을 목적으로 정보주

82) Article 23(Data protection by design and by default) 1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

체로부터 개인정보를 수집할 때에는 제3자로의 제공을 이용 목적으로 한다는 사실, 제3자에게 제공될 개인데이터의 항목, 제3자로의 제공 수단 또는 방법, 정보주체의 요구가 있으면 당해 본인이 식별되는 개인데이터의 제3자로의 제공이 정지된다는 사실 등을 알리도록 되어 있으나 제공받을 제3자를 특정하도록 요구하고 있지는 않다.

2012년 EU Regulation 제14조	일본 개인정보보호법 제23조
제14조(정보주체에 대한 정보) 1. 정보주체와 관련된 개인정보가 수집되는 경우 개인정보처리자는 정보주체에게 다음 각 호의 정보를 제공해야 한다. : (a) 개인정보처리자 그리고 가능한 경우 개인정보처리자의 대리인 및 정보보호 담당자의 신원 및 연락처; (b) 개인정보의 처리 목적. 개인정보가 제6조제1항 (b)에 의해서 처리되는 경우에는 해당 계약의 조건 또는 개인정보가 제6조제1항 (f)에 의해서 처리되는 경우에는 개인정보처리자	제23조(제3자 제공의 제한) ① (생 략) ② 개인정보취급사업자는 제3자에게 제공된 개인 데이터에 관하여, 본인의 요구에 응하여 당해 본인이 식별되는 개인 데이터의 제3자로의 제공을 정지하고 있는 경우에 있어, 다음 각 호에 게재된 사항에 관하여 미리 본인에게 통지 또는 본인이 용이하게 알 수 있는 상태로 하고 있는 경우에는 전항의 규정에 상관없이 당해 개인데이터를 제3자에 제공할 수 있다. 1. 제3자로의 제공을 이용

가 추구하는 정당한 이득을 포함한다. (c) 개인정보가 보관되는 기간; (d) 정보주체와 관련된 개인정보의 접근 및 수정 또는 삭제를 요청하거나 이러한 개인정보의 처리를 반대할 수 있는 권리의 존재 여부; (e) 감독기관에게 불만 사항을 제기할 수 있는 권리와 감독기관에 과한 상세한 연락처 정보; (f) 개인정보 수령인 또는 수령인의 범주; (g) 해당되는 경우, 유럽집행위원회의 적절한 결정에 따라 제3국이나 국제기구가 제공하는 보호조치 하에서 개인정보처리자가 제3국이나 국제기구에 개인정보를 이전하려고 하는 의도; (h) 개인정보가 수집되는 특정한 상황 하에서 정보주체와 관련된 개인정보의 공정한 처리를 보증하기	목적으로 한다는 사실 2. 제3자에게 제공될 개인데이터의 항목 3. 제3자로의 제공 수단 또는 방법 4. 정보주체의 요구가 있으면 당해 본인이 식별되는 개인데이터의 제3자로의 제공이 정지된다는 사실

위해 필요한 그 밖의 정보 2~4. (생 략)	

제4절 개인정보처리 위탁 시 공개의무 완화 (제26조제2항)

1. 현황 및 문제점

개인정보보호법은 개인정보처리자가 제3자에게 개인정보 처리업무를 위탁하는 경우 개인정보처리자 즉 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하도록 교육의무와 관리·감독의무를 부여하는 한편, 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 보도록 규정하고 있다.

그밖에 개인정보처리자는 개인정보의 처리 업무를 위탁하는

경우에는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 “수탁자”라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 하고, 개인정보처리자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알리도록 요구하고 있다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.

이에 따라 대통령령은 개인정보처리자가 개인정보 처리 업무를 위탁하는 경우에는 개인정보처리자의 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재하도록 하고 있으며, 인터넷 홈페이지에 게재할 수 없는 경우에는 개인정보처리자의의 사업장등의 보기 쉬운 장소에 게시하는 방법, 관보(개인정보처리자가 공공기관인 경우만 해당한다)나 위탁자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조 제1호 가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법, 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 싣는 방법, 재화나 용역을 제공하기 위하여 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법으로 위탁하는 업무의 내용과 수탁자를 공개하도

록 규정하고 있다. 다만, 개인정보처리자가 과실 없이 위탁하는 업무의 내용과 수탁자를 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 하고, 인터넷 홈페이지를 운영하지 아니하는 경우에는 사업장 등의 보기 쉬운 장소에 30일 이상 게시하도록 규정하고 있다.[83]

그 결과 개인정보처리자는 개인정보처리가 수반되는 업무를 위탁할 때에는 미리 인터넷 홈페이지 등을 통해 위탁하는 업무의 내용과 수탁자의 신원을 공개해야 한다. 그러나 위탁업무의 내용 또는 수탁자의 신원을 공개할 경우 기업의 영업비밀 유출, 수탁자의 사생활 침해 등과 같은 다른 법익을 침해하는 문제가 발생한다. 또, 개인정보처리가 수반되는 업무를 계속적으로 위탁하는 것이 아니라 1회에 한해서 단기간 위탁하거나 두, 세 사람만의 개인정보가 처리되도록 업무를 위탁하는 경우에도 위탁하는 업무의 내용과 수탁자를 인터넷 홈페이지, 신문 등을 통해 정보주체에게 알려야 하기 때문에 불필요하게 과도한 비용이 소요되고 이해당사자가 아닌 정보주체에게까지 알려야 하는 부담이 있다.

2. 개정방향

83) 개인정보보호법 시행령 제28조 참조.

개인정보처리자가 개인정보 처리업무가 수반되는 업무를 제3자에게 위탁하고자 하는 때에는 원칙적으로 위탁하는 업무의 내용과 수탁자를 공개하도록 하되, 영업 비밀을 침해할 우려가 있거나 수탁자의 사생활을 침해할 우려가 있는 경우에는 대통령령이 정하는 바에 따라 공개의무를 면제하도록 해야 한다. 예컨대, 극비로 진행해야 하는 M&A업무, 법률·경영·회계자문, 고객 분석 업무, 신변보호업무, 컨벤션업무, 국가비밀처리, 보험모집업무 등이 이에 속할 수 있다.

또한, 개인정보처리업무의 위탁이 1회에 그쳐 위탁기간이 매우 짧거나 위탁 처리되는 개인정보의 수가 적어 공개의 실익이 크지 않은 경우로써 대통령령으로 정한 경우에는 공개하지 않을 수 있도록 해야 한다. 다만, 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 현행과 마찬가지로 1회성으로 개인정보 처리업무를 위탁하더라도 해당 위탁업무의 내용(마케팅 목적의 개인정보 수집업무 위탁 등)과 수탁자를 고지하도록 한다.

개정안 신·구 대조표

현 행	개 정 안
제26조(업무위탁에 따른 개인정보의 처리 제한) ①	제26조(업무위탁에 따른 개인정보의 처리 제한) ①

개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다. 1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 2. 개인정보의 기술적·관리적 보호조치에 관한 사항 3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항 ② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 “위탁자”라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 “수탁자”라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.	개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다. 1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 2. 개인정보의 기술적·관리적 보호조치에 관한 사항 3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항 ② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 “위탁자”라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 “수탁자”라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다. 다만, 위탁하는 업무의 내용 또는 수탁자의 이름이 공개될 경우 비밀, 사생활 등의 침해 우려가

	큰 경우 또는 위탁기간이 짧거나 위탁 처리되는 개인정보의 수가 적어 공개의 실익이 크지 않은 경우로써 대통령령으로 정한 경우에는 공개하지 않을 수 있다.
③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.	③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.
④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.	④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.
⑤ 수탁자는 개인정보처리	⑤ 수탁자는 개인정보처리

자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다. ⑥ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다. ⑦ 수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.	자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다. ⑥ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다. ⑦ 수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.

3. 외국사례

일본 개인정보보호법은 개인정보취급사업자가 개인 데이터 취급업무의 전부 또는 일부를 위탁하는 경우에는 그 취급이 위탁된 개인 데이터의 안전한 관리가 도모되도록 위탁을 받은 자에 대한 필요하고도 적절한 감독을 하여야 한다고 하여 수

탁자에 대한 관리·감독 의무를 규정하고 있으나, 위탁업무의 내용 또는 수탁자의 신원을 공개할 의무는 부여하고 있지 않다.

한편, EU 개인정보보호법안은 정보주체의 개인정보를 충분히 보호할 수 있는 기술적·관리적 조치능력이 있는 수탁자를 선정할 의무, 개인정보처리자의 지시사항과 수탁자의 의무사항을 구속력 있는 계약이나 법률행위로 하고 그 내용을 문서화할 의무, 수탁자의 불법행위에 대하여 사용자로서의 책임을 질 의무 등을 개인정보처리자에게 부담지우고 있으나, 일본 개인정보보호법과 마찬가지로 위탁업무의 내용 또는 수탁자의 신원을 공개할 의무를 부여하고 있지는 않다. 다만, 개인정보처리자가 정보주체에 관한 개인정보를 수집하는 경우에는 개인정보처리자의 신원과 연락처 외에 가능한 경우에는 개인정보처리자의 대리인 및 정보보호 담당자(the controller's representative and of the data protection officer)의 신원 및 연락처도 알려 주도록 요구하고 있다.[84]

---

84) Article 14 (Information to the data subject) 1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:
(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;
(b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
(c) the period for which the personal data will be stored;

2012년 EU Regulation 제26조	일본 개인정보보호법 제22조
제26조(처리자) 1. 개인정보 처리자는 자신을 대신해서 개인정보가 처리되는 경우 해당 개인정보의 처리가 이 법의 요구조건을 충족하고 정보주체의 권리를 보호하는 방식으로 기술적·관리적 보호조치가 적절하게 이행한다는 것을 충분히 보증할 수 있는 프로세서(수탁자)를 선정하여야 하고, 기술적·관리적 보호조치와 관련하여 정보주체의 권리보호를 보장하여야 한다.	제22조(위탁처의 감독) 개인정보취급사업자는 개인 데이터의 취급의 전부 또는 일부를 위탁하는 경우에는 그 취급이 위탁된 개인 데이터의 안전관리가 도모되도록 위탁을 받은 자에 대한 필요하고 적절한 감독을 행하여야 한다.

(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;
(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;
(f) the recipients or categories of recipients of the personal data;
(g) where applicable, that the controller intends to transfer to a third country or international organization and on the level of protection afforded by that third country or international organization by reference to an adequacy decision by the Commission;
(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.
2~8 (생 략)

2. 프로세서가 개인정보를 처리하는 경우 해당 개인정보처리는 프로세서를 구속하는 계약이나 법률행위에 기초하여야 하며 특히 해당 계약이나 법률행위에는 다음과 같은 사항이 포함되어야 한다. (a) 수탁자는 개인정보처리자의 지시에 따라서만 일을 처리한다. 특히 개인정보의 이전(transfer)이 금지되는 경우에는 반드시 개인정보처리자의 지시에 따른다. (b) 수탁자는 비밀준수의무가 부여되어 있거나 법률상 비밀준수의무를 지고 있는 직원만을 고용해야 한다. (c) 수탁자는 제30조(기술적·관리적 보호조치)에 의해서 요구되는 모든 보호조치를 취해야 한다. (d) 수탁자는 개인정보처리자의 사전 동의를 얻은 후에만 개인정보처리에 있어서 다른 사람의 협력을 구	

한다. (e) 수탁자는 개인정보처리자와의 합의를 통해 정보주체의 권리행사에 필요한 개인정보처리자의 의무 이행을 위한 기술적·관리적인 요건을 정한다. (f) 수탁자는 개인정보처리자가 제30조에서부터 제34조에 따른 의무규정을 준수하도록 개인정보처리자를 지원한다. (g) 개인정보 처리업무가 끝난 후에는 모든 결과를 개인정보처리자에게 넘겨주고 더 이상 개인정보를 처리하지 않는다. (h) 본조에서 규정하고 있는 의무의 준수 여부를 감독하는데 필요한 모든 정보를 개인정보처리자와 관계 감독당국에게 제공한다. 3. 개인정보처리자와 프로세서는 제2항에 따른 개인정보처리자의 지시사항과 프로세서의 의무사항을 서면으로 문서화해야 한다. 4. 프로세서가 개인정보처	

리자의 지시 없이 개인정보를 처리하는 경우 처리자는 이러한 처리와 관련하여 개인정보처리자로 간주되며 제24조에서 규정한 공동 개인정보처리자에 관한 규정이 적용된다. 5. 유럽연합 집행위원회는 제1항에서 언급한 프로세서와 관련된 책임, 의무, 업무 등에 대한 기준 및 요건과 사업체 집단(group of undertakings) 내에서의 개인정보 처리를 용이하게 해 주는 조건 특히 관리 및 보고 목적을 위한 조건을 규정하기 위해 제86조에 따라 위임된 법안을 채택할 수 있는 권한을 부여받아야 한다.	

제5절 일부적용 제외의 명확화 및 빅데이터 문제 해소 (제58조)

1. 현황 및 문제점

개인정보보호법은 제58조에서 이 법의 일부 적용 제외에 대해서 규정하고 있으나 적용제외의 범위, 대상 등이 분명하지 않고, 또 적용제외의 범위, 대상이 개인정보를 처리하고 있는 실제 환경과 맞지 않아 개인정보처리자 자신은 물론 정보주체의 사회·경제 활동을 위축시킬 우려가 있다.

예컨대, 개인정보보호법은 언론사, 종교단체, 정당이 그 고유 목적을 달성하기 위하여 수집·이용하는 개인정보에 대하여는 개인정보보호법의 일부 적용을 면제하고 있다. 그런데, 이 경우 개인정보보호법의 일부 적용이 면제되는 개인정보처리의 목적이 「언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보」로 되어 있어 면제되는 개인정보의 범위, 대상이 애매하고 '고유 목적'이라는 의미도 추상적이라는 비판을 받을 우려가 있다.

한편, 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 개인정보보호법 제15조

(개인정보 수집・이용), 제30조(개인정보 처리방침의 수립 및 공개) 및 제31조(개인정보 보호책임자의 지정)를 적용하지 아니하여 회원정보의 수집・이용은 자유로우나 제17조(개인정보의 제공)의 적용은 면제되지 아니하여 친목단체 회원들 간에도 고지・동의 절차를 거치지 아니하면 회원명부를 배포할 수 없다.

한편, 개인정보보호법은 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보에 대하여는 제3장부터 제7장까지의 적용을 면제하고 있으나, 민간부문에서 통계처리, 과학연구, 역사적 기술을 목적으로 처리되는 개인정보에 대하여는 개인정보보호법의 일부 적용이 면제되지 않고 있다.[85] 이에 따라 최근 빅데이터 환경에서 전 세계적으로 정보의 활용가치가 강조되고 있으나 현행 개인정보보호법 하에서는 통계처리, 과학연구, 역사적 기술과 같은 공익 목적으로도 정보주체의 동의가 없는 한 데이터의 활용이 불가능하다. 그러나 이

85) 개인정보보호법 제18조제2항 제4호는 '통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우'에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다고 규정하고 있다. 그러나 제18조에 의해서 개인정보를 통계작성, 학술연구 등의 목적으로 이용 또는 제공하기 위해서는 '특정 개인을 알아볼 수 없는 형태'로 해서 개인정보를 제공해야 하기 때문에 동의 면제는 법률상 아무 의미가 없다. 개인정보는 '특정 개인을 알아볼 수 없는 형태'로 전환한 순간 개인정보보호법상의 개인정보가 아니므로 제18조제2항 제4호가 없더라도 정보주체의 동의 없이 얼마든지 수집・이용・제공이 가능하기 때문이다.

와 같은 목적의 개인정보 수집과 활용은 사생활 침해 위험이 상대적으로 낮고 이에 비하여 공익성은 크다. 하지만 정보주체의 동의를 받지 못하거나 정보주체가 동의를 거부하면 활용할 수 없게 된다. 특히 의료정보, 건강정보, 시청각 습관, 소비·구매 트렌드 등은 학술적 연구가치가 높지만 정보주체의 동의를 받기는 쉽지 않다.

2. 개정방향

개인정보보호법의 일부 적용이 면제되는 범위를 1) 언론사의 취재·보도, 2) 종교단체의 선교, 3) 정당의 선거 입후보자 추천 등으로 명확하게 한정하여 해석상 논란을 없애고, 또한 친목단체를 운영하기 위하여 개인정보를 처리하는 경우에는 개인정보 수집·이용 규정(제15조)뿐만 아니라 제3자 제공 규정(제17조)도 적용을 면제하여 친목단체의 회원 간에는 개인정보가 자유롭게 수집·이용·제공될 수 있도록 하여야 함으로써 친목단체 회원들 간의 개인정보 이용·제공·공유·공개 여부에 대해서는 회칙 등 자율규제에 맡겨야 한다.

또한, 사생활 침해 가능성이 낮으면서도 사회적·공익적 이익이 큰 통계처리·과학연구·역사적 기술 목적의 개인정보처리에 대하여도 정보주체의 개인정보에 대한 기술적·관리적 보호조치 등의 의무이행을 조건으로 제한적으로 허용할 필요가

있다. 즉, 통계처리·과학연구·역사적 기술 목적의 개인정보 처리는 정보주체의 동의 없이도 가능하게 하되, 해당 정보가 특정 개인의 것이라는 사실을 알게 하는 정보(이름, 고유식별번호, 주소, 전화번호 등)는 원칙적으로 다른 정보와 분리하여 처리·보관하도록 하고, 목적을 위하여 필요한 범위에서 최소한의 기간에 최소한의 개인정보만을 처리하게 하여야 하며, 개인정보의 안전한 관리를 위하여 필요한 기술적·관리적 및 물리적 보호조치, 개인정보의 처리에 관한 고충처리, 그 밖에 개인정보의 적절한 처리를 위하여 필요한 조치를 마련하도록 하여야 한다.

개정안 신·구 대조표

현 행	개 정 안
제58조(적용의 일부 제외) ① 다음 각 호의 어느 하나에 해당하는 개인정보에 관하여는 제3장부터 제7장까지를 적용하지 아니한다. 1. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보 2. 국가안전보장과 관련된	제58조(적용의 일부 제외) ① 다음 각 호의 어느 하나에 해당하는 개인정보에 관하여는 제3장부터 제7장까지를 적용하지 아니한다. 1. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보 2. 국가안전보장과 관련된

정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보	정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보
3. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보	3. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보
4. 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유목적을 달성하기 위하여 수집·이용하는 개인정보	4. 언론사의 취재·보도, 종교단체의 선교, 정당의 선거 입후보자 추천을 목적으로 수집·이용하는 개인정보
② 제25조제1항 각 호에 따라 공개된 장소에 영상정보처리기기를 설치·운영하여 처리되는 개인정보에 대하여는 제15조, 제22조, 제27조제1항·제2항, 제34조 및 제37조를 적용하지 아니한다.	② 제25조제1항 각 호에 따라 공개된 장소에 영상정보처리기기를 설치·운영하여 처리되는 개인정보에 대하여는 제15조, 제22조, 제27조제1항·제2항, 제34조 및 제37조를 적용하지 아니한다.
③ 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조, 제30	③ 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조, 제17

조 및 제31조를 적용하지 아니한다.	조, 제30조 및 제31조를 적용하지 아니한다.
<신 설>	④ 통계처리, 과학연구, 역사적 기술을 목적으로 처리되는 개인정보에 대하여는 제15조에서 제18조, 제21조, 제23조에서 제25조를 적용하지 아니한다.
④ 개인정보처리자는 제1항 각 호에 따라 개인정보를 처리하는 경우에도 그 목적을 위하여 필요한 범위에서 최소한의 기간에 최소한의 개인정보만을 처리하여야 하며, 개인정보의 안전한 관리를 위하여 필요한 기술적·관리적 및 물리적 보호조치, 개인정보의 처리에 관한 고충처리, 그 밖에 개인정보의 적절한 처리를 위하여 필요한 조치를 마련하여야 한다.	⑤ 개인정보처리자는 제1항 각 호 및 제4항에 따라 개인정보를 처리하는 경우에도 그 목적을 위하여 필요한 범위에서 최소한의 기간에 최소한의 개인정보만을 처리하여야 하며, 개인정보의 안전한 관리를 위하여 필요한 기술적·관리적 및 물리적 보호조치, 개인정보의 처리에 관한 고충처리, 그 밖에 개인정보의 적절한 처리를 위하여 필요한 조치를 마련하여야 한다.
<신 설>	⑥ 개인정보처리자가 제4항에 따라 개인정보를 처

	리할 때에는 특정 개인을 알아 볼 수 없게 하면 그 목적을 달성할 수 없는 경우를 제외하고 해당 정보가 특정 개인의 것이라는 사실을 알게 하는 정보(이름, 고유식별번호, 주소, 전화번호 등)를 다른 정보와 분리하여 별도로 처리하거나 보관하여야 한다. 이 경우 목적을 달성할 수 없는 경우라는 입증책임은 개인정보처리자가 부담한다.

3. 외국사례

일본 개인정보보호법은 우리나라 개인정보보호법과 마찬가지로 보도기관(언론기관), 종교단체, 정치단체에 대한 일부 적용을 규정하는 외에 저술자, 학술연구 기관·단체·개인에 대하여도 일부 적용을 면제하고 있다. 그러나 일부 적용 면제의 범위 또는 대상은 각각 보도목적, 저술목적, 학술연구목적, 종교

활동, 정치활동 등으로 매우 넓게 규정되어 있다. 뿐만 아니라 정치 분야에 있어서도 “정당”으로 한정하지 않고 “정치단체”로 하여 제도권 정당과 제도권 밖의 정치단체 간의 차별을 없앴다. 다만, 친목단체에 대하여는 우리나라와 달리 일부 적용 면제를 규정하고 있지 않다.[86] 또한, 형사사건이나 소년보호사건과 관련된 재판, 검찰관·검찰사무관·사법경찰관이 행한 처분, 형이나 보호처분의 집행, 갱생긴급보호나 사면 등과 관련하여 행정기관이 보관하고 있는 보유개인정보에 대해서는 「행정기관이 보유하는 개인정보보호법」의 일부 적용이 면제된다.[87]

2012년 EU Regulation은 공공의 안녕(public security), 범죄의 예방·수사·내사 및 기소, 금융·예산·조세 문제와 시장의 안정 및 통합 보호를 포함하여 유럽연합 또는 회원국의 중요한 금융 또는 재정상의 이익과 그 밖의 공공적 이익, 법률에 의해서 규제를 받고 있는 특수 전문직의 직업윤리 침해에 대한 예방·수사·내사 및 기소, 그 밖에 정보주체나 다른 사람의 권리와 자유 보호 등을 위하여, 필요하고도 적절한 범위 내에서 제5조[88] (a)에서 (e)까지, 제11조에서 제20조까지[89], 제32

86) 일본 개인정보보호법 제50조 참조.
87) 일본 행정기관이 보유하는 개인정보보호법 제45조 참조.
88) 제5조(개인정보의 처리 원칙)
89) 제11조(개인정보처리방침의 투명한 공개 및 개인정보처리에 관한 정보의 제공), 제12조(정보주체의 권리행사를 위한 절차 및 방법), 제13조(개인정보를 제공받는 자와 관련한 정보주체의 권리), 제14조(정보주체에 대한 정보 제공), 제15조(자기에 관한 정보에 대한 정보주체의 접근권),

조[90]에서 규정된 의무와 권리의 범위를 유럽연합 또는 회원국의 법률로 제한할 수 있다고 규정하고 있다.

또한, 2012년 EU Regulation은 특별한 개인정보의 처리라고 하여 언론보도 및 표현의 자유를 위한 개인정보처리(제80조), 예방의학・직업병의학・의료진단・치료・처치・건강관리 등을 위한 건강정보의 처리(제81조), 고용관계에서의 개인정보처리(제82조), 역사・통계・과학연구 목적의 개인정보처리(제83조), 교회 및 종교단체의 개인정보처리(제85조) 등에 대한 일부적용 제외를 규정할 수 있도록 하거나 규정하도록 요구하고 있다.

첫째, 회원국은 개인정보 보호권과 표현의 자유를 조화시키기 위하여 오로지 언론 목적 또는 예술적・문학적 표현 목적으로 처리되는 개인정보에 대하여는 제II장의 일반원칙, 제III장의 정보주체 권리, 제IV장의 개인정보처리 및 수탁자, 제V장의 제3국 및 국제기구로의 개인정보 이전, 제VI장의 독립적인 감독기관, 제VII장의 협력 및 일관성 보증 등에 대해 예외나 부분 수정을 규정할 수 있다.[91]

제16조(정정 요구권), 제17조(잊혀 질 권리 및 삭제 요구권), 제18조(정보이전 요구권), 제19조(처리정지 요구권), 제20조(프로파일링에 근거한 조치)

90) 제32조(개인정보침해에 대항 통지의무)

91) Article 80 (Processing of personal data and freedom of expression)
1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organizations in Chapter V, the independent supervisory

둘째, 건강과 관련한 개인정보는 제9조(2)항에서 규정한 바에 따라 정보주체의 정당한 권리를 보호하기 위한 적절하고도 구체적인 조치를 규정하고 있는 유럽연합 또는 회원국의 법률에 따라 처리되어야 하며, (a) 업무상 비밀준수의무를 지는 건강 전문 등이 처리하는 경우로써 예방 의학·직업병 의학·의료진단·치료·처치·건강관리 등을 위한 목적, (b) 국경을 넘나드는 건강 위협에 대한 방어, 의약품 및 의료용품의 품질이나 안전성 보증 등과 같은 공중보건 분야에서의 공공이익 보호 목적, (c) 건강보험 시스템에서 분쟁해결을 위해 사용되는 절차의 품질 및 비용효율성 보장 등 사회적 이익보호와 관련된 영역에서의 공공이익 보호 목적 등을 위해서 처리될 수 있어야 한다. 또한, 진단방법 개선, 유사질병 구분, 치료를 위한 연구준비 등을 위해 정리된 환자기록과 같이 역사, 통계, 과학연구 목적을 위해 필요한 건강정보의 처리는 제83조에서 규정하고 있는 조건과 안전조치에 따라서 처리될 수 있다.[92]

---

authorities in Chapter VI and on co-operation and consistency in Chapter VII for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.

2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.

92) Article 81 (Processing of personal data concerning health) 1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall

셋째, 회원국들은 이 법안의 범위 내에서 고용관계에 있어서 (a) 채용, (b) 법률 또는 단체협약상의 의무면제, 노무의 관리·계획 및 조직, 작업장에서의 건강 및 안전 등과 같은 고용계약의 이행, (c) 개인별 또는 집단적으로 고용과 관련된 권리 및 혜택의 행사와 향유, (d) 고용관계의 해지 등을 위해 근로자의 개인정보처리를 규율하는 특별한 원칙을 회원국의 법률로 채택할 수 있다.[93]

---

provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for:

(a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or

(b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or

(c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.

2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying other reasons of public interest in the area of public health as referred to in point (b) of paragraph 1, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

넷째, (a) 정보주체의 신원확인을 허용하지 아니하면 역사, 통계, 과학연구의 목적을 달성할 수 없는 경우나, (b) 정보주체의 신원을 확인해 주거나 확인을 가능하게 해주는 정보를 다른 정보와 분리해서 별도로 보관하더라도 이와 같은 방법을 통해 역사, 통계, 과학연구의 목적을 달성할 수 있는 경우에는 이 법안의 범위 내에서 역사, 통계, 과학연구 목적으로 개인정보를 처리할 수 있다. 또한, 역사, 통계, 과학연구를 수행하는 기관은 (a) 제7조에 따라 정보주체의 동의를 받은 경우, (b) 정보주체의 이익, 기본 권, 자유가 역사, 통계, 과학연구 목적의 이익보다 우월하지 아니한 경우로써 연구결과를 제시하기 위해 또는 연구를 용이하게 하기 위해 개인정보의 공개가 필요한 경우, (c) 정보주체가 이미 해당 정보를 공개한 경우에는

93) Article 82(Processing in the employment context) 1. Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organization of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.
2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

개인정보를 공표할 수 있다.[94]

다섯째, 이 법안이 시행되는 시점에서 회원국 내의 교회나 종교단체가 개인정보의 처리와 관련하여 개인을 보호하기 위한 포괄적인 규범(rules)을 가지고 있는 경우, 이 법안의 규정에 배치되지 않는 한 해당 규범들은 계속해서 적용될 수 있다. 그러나 해당 교회나 종교단체는 이 법안의 제VI장에 따라 독립적인 감독기관을 갖추고 있어야 한다.[95]

---

94) Article 83(Processing for historical, statistical and scientific research purposes) 1. Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:
(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;
(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.
2. Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if:
(a) the data subject has given consent, subject to the conditions laid down in Article 7;
(b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or
(c) the data subject has made the data public.
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.

95) Article 85(Existing data protection rules of churches and religious associations) 1. Where in a Member State, churches and religious

이상과 같이 2012년 EU Regulation은 개인정보보호법의 일부 적용을 면제할 수 있는 다양한 상황을 준비하고 있지만, 우리나라와 달리 정당이나 친목단체에 대한 개인정보보호법의 일부 적용 제외는 규정하고 있지 않다.

2012년 EU Regulation 제26조	일본 개인정보보호법 제50조
제21조(제한) 1. 민주주의 사회에서 다음 각 호의 사항을 보장하기 위하여 필요하고도 적절한 범위 내에서 제5조 (a)에서 (e)까지, 제11조에서 제20조까지, 제32조에서 규정된 의무와 권리의 범위를 유럽연합 또는 회원국의 법률로 제한할 수 있다. (a) 공공의 안녕; (b) 범죄의 예방, 수사, 내	제50조(적용제외) ① 개인정보취급사업자 중 다음 각 호에 게재된 자에 대해서는 그 개인정보를 취급하는 목적의 전부 또는 일부가 각각 다음의 각호에 규정된 목적인 경우에는 전장(前章)의 규정을 적용하지 아니한다. 1. 방송기관, 신문사, 통신사 그 밖의 보도기관(보도를 업으로 하는 개인을 포

associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 shall provide for the establishment of an independent supervisory authority in accordance with Chapter VI of this Regulation.

사 및 기소; (c) 금융·예산·조세 문제와 시장의 안정 및 통합 보호를 포함하여 유럽연합 또는 회원국의 중요한 금융 또는 재정상의 이익과 그 밖의 공공적 이익 ; (d) 법률에 의해서 규제를 받고 있는 특수 전문직의 직업윤리 침해에 대한 예방, 수사, 내사 및 기소; (e) 앞의 (a), (b), (c), (d)에서 규정하고 있는 공적 권한 행사와 관련된 감시, 조사, 규제 기능; (f) 정보주체나 다른 사람의 권리와 자유 보호; 2. 제1항에서 언급한 법률적 조치에는 최소한 개인정보처리자의 처리 및 결정에 의해 추구되는 목적에 관한 구체인 규정이 포함되어야 한다.	함한다) - 보도 목적 2. 저술을 업으로 하는 자 - 저술에 이용하는 목적 3. 대학 그밖에 학술연구를 목적으로 하는 기관 혹은 단체 또는 그에 속하는 자 - 학술연구의 목적 4. 종교단체 - 종교 활동(이에 부수하는 활동을 포함한다)의 목적 5. 정치단체 - 정치활동(이에 부수하는 활동을 포함한다)의 목적 ② 전항 제1호에서 규정한 「보도」란 불특정 다수의 자에 대하여 객관적 사실을 사실로서 알리는 일(이에 근거하여 의견 또는 견해를 나타내는 것을 포함한다)을 말한다. ③ 제1항 각 호에 게재된 개인정보취급사업자는 개인데이터의 안전관리를 위하여 필요하고 적절한 조치, 개인정보의 취급에 관한 고충의 처리 기타의 개인정보의 적정한 취급을 확보하기 위하여 필요한

	조치를 스스로 강구하고 당해 조치의 내용을 공표하도록 노력하여야 한다.

Ⅵ. 개인정보 보호위원회의 권한 및 독립성 강화

제1절 보호위원회의 인사·예산 등 독립성 강화 (제7조)

1. 현황 및 문제점

개인정보보호법상 보호위원회는 대통령 소속으로 되어 있고, 그 권한에 속하는 업무를 독립하여 수행하도록 규정되어 있다. 그러나 독립기구로서의 성격에 맞지 않게 보호위원회는 소속 직원들에 대한 인사권도 없고 예산권도 확보되어 있지 않다. 또한 보호위원회의 직원은 상당수가 파견 직원으로 구성되어 있으며 보호위원회 소속의 자체 직원은 소수에 불과하다. 그밖에 보호위원회 위원에 대하여는 임기는 있으나 명확한 신분보장 규정이 없으며, 이해관계 사건에 대한 제척·기피·회피 제도도 도입되어 있지 아니하다.

법률상 그 업무를 독립하여 수행하도록 규정되어 있더라도 인사권과 예산권이 독립되어 있지 아니하면 독립적인 권한 행사는 현실적으로 어렵다고 할 수 있다. 또한 보호위원회라는 기구 자체의 독립성도 중요하지만, 그 기구를 구성하고 있는 구성원인 보호위원회의 위원과 직원들이 내·외부로부터의 압력이나 유혹에 흔들리지 않고 독립적으로 업무를 수행할 수

있도록 지원하는 제도적인 장치도 중요하다. 그러나 현행 개인정보보호법은 명분상으로만 그 권한에 속하는 권한을 독립적으로 수행한다고 선언하고 있을 뿐, 보호위원회와 그 구성원이 자율성(autonomy)과 독립성(independence)을 가지고 임무를 수행할 수 있는 실천적인 장치는 거의 마련되어 있지 않다.

2. 개정방향

보호위원회가 국제적으로 인정받는 개인정보보호 감독기구(DPA)로 활동하기 위해서는 자체 임무 및 기능 수행에 필요한 자율성과 독립성을 충분히 보장받아야 한다. 이 때 자율성이란 법률적으로나 실질적으로 다른 기관의 승인을 구하지 않고 행동을 계획·실행할 수 있는 권한을 부여받고 있어야 하는 것을 의미하고, 독립성이란 정치권이나 행정부의 영향을 받지 않고 자유롭게 운영할 수 있고 기득권을 배격할 수 있어야 하는 것을 의미한다.

먼저, 보호위원회의 자율성과 독립성 강화를 위해 보호위원회 위원장을 현행 비상임에서 정무직 공무원으로 격상하고 국회의 인사 청문을 거쳐 대통령이 임명하도록 한다. 위원은 현행 15명에서 9명으로 축소하고, 개인정보에 관하여 전문적인 지식과 경험이 있고 개인정보보호 업무를 공정하고 독립적으로 수행할 수 있다고 인정되는 사람 중에서 국회가 선출한 3명과

대통령 및 대법원장이 각각 지명한 3명을 대통령이 임명하고, 금고 이상의 형의 선고에 의하지 아니하고는 본인의 의사에 반하여 면직되지 아니하도록 하여 신분을 보장하도록 한다.

보호위원회 사무국을 사무처로 승격하고, 사무국 직원에 대한 인사권을 위원장에게 부여하며, 예산도 보호위원회가 독립하여 편성하고 국회에 요구하도록 한다. 또한, 업무를 효율적으로 수행하기 위하여 보호위원회에 소위원회를 둘 수 있도록 하고, 보다 전문적인 심의·의결이 가능하도록 소위원회에는 심의사항을 연구·검토하기 위하여 분야별 전문위원회를 둘 수 있도록 한다.

개정안 신·구 대조표

현 행	개 정 안
제7조(개인정보 보호위원회) ① 개인정보 보호에 관한 사항을 심의·의결하기 위하여 대통령 소속으로 개인정보 보호위원회(이하 “보호위원회”라 한다)를 둔다. 보호위원회는 그 권한에 속하는 업무를 독립하여 수행한다. ② 보호위원회는 위원장 1명, 상임위원 1명을 포함	제7조(개인정보 보호위원회) ① 개인정보 보호에 관한 사항을 심의·의결하기 위하여 대통령 소속으로 개인정보 보호위원회(이하 “보호위원회”라 한다)를 둔다. 보호위원회는 그 권한에 속하는 업무를 독립하여 수행한다. ② 보호위원회는 위원장 1명과 상임위원 1명을 포함

한 15명 이내의 위원으로 구성하되, 상임위원은 정무직 공무원으로 임명한다.	한 9명 이내의 위원으로 구성하되, 위원장과 상임위원은 정무직 공무원으로 임명한다.
③ 위원장은 위원 중에서 공무원이 아닌 사람으로 대통령이 위촉한다.	③ 위원장은 대통령이 임명한다. 이 경우 위원장은 국회의 인사 청문을 거쳐야 한다.
④ 위원은 다음 각 호의 어느 하나에 해당하는 사람을 대통령이 임명하거나 위촉한다. 이 경우 위원 중 5명은 국회가 선출하는 자를, 5명은 대법원장이 지명하는 자를 각각 임명하거나 위촉한다.	④ 위원은 개인정보에 관하여 전문적인 지식과 경험이 있고 개인정보보호 업무를 공정하고 독립적으로 수행할 수 있다고 인정되는 사람 중에서 다음 각 호의 사람을 대통령이 임명한다.
1. 개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람	1. 국회가 선출하는 3명(상임위원 1명을 포함한다)
2. 개인정보처리자로 구성된 사업자단체로부터 추천을 받은 사람	2. 대통령이 지명하는 3명
3. 그 밖에 개인정보에 관한 학식과 경험이 풍부한 사람	3. 대법원장이 지명하는 3명
⑤ 위원장과 위원의 임기는 3년으로 하되, 1차에	⑤ 위원장과 위원의 임기는 3년으로 하되, 1차에

한하여 연임할 수 있다.	한하여 연임할 수 있다. 위원은 금고 이상의 형의 선고에 의하지 아니하고는 본인의 의사에 반하여 면직되지 아니한다. 다만, 위원이 신체상 또는 정신상의 장애로 직무수행이 극히 곤란하게 되거나 불가능하게 된 경우에는 전체 위원 3분의 2 이상의 찬성에 의한 의결로 퇴직하게 할 수 있다.
⑥ 보호위원회의 회의는 위원장이 필요하다고 인정하거나 재적위원 4분의 1 이상의 요구가 있는 경우에 위원장이 소집한다.	⑥ 보호위원회의 회의는 위원장이 필요하다고 인정하거나 재적위원 4분의 1 이상의 요구가 있는 경우에 위원장이 소집한다.
⑦ 보호위원회는 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결한다.	⑦ 보호위원회는 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결한다.
⑧ 보호위원회의 사무를 지원하기 위하여 보호위원회에 사무국을 둔다.	⑧ 보호위원회의 사무를 지원하기 위하여 보호위원회에 사무처를 둔다. 사무처에 사무처장 1명과 필요한 직원을 두되 사무처장은 위원회의 심의를 거쳐 위원장의 제청으로 대통령

	이 임명하고, 소속 직원 중 5급 이상 공무원 또는 고위공무원단에 속하는 일반직공무원은 위원장의 제청으로 대통령이 임명하며, 6급 이하 공무원은 위원장이 임명한다.
<신 설>	⑨ 보호위원회는 그 업무를 효율적으로 수행하기 위하여 소위원회를 둘 수 있고, 소위원회에는 심의사항을 연구·검토하기 위하여 분야별 전문위원회를 둘 수 있다.
<신 설>	⑩ 보호위원회는 예산을 독립하여 편성하고 국회에 요구한다. 이 경우 위원장은 위원회의 예산 관련 업무를 수행할 때 「국가재정법」 제6조제3항에 따른 중앙관서의 장으로 본다.
⑨ 제1항부터 제8항까지에서 규정한 사항 외에 보호위원회의 조직과 운영에 필요한 사항은 대통령령으로 정한다.	⑪ 제1항부터 제10항까지에서 규정한 사항 외에 보호위원회, 소위원회 및 전문위원회의 조직과 운영에 필요한 사항은 대통령령으로 정한다.

3. 외국사례

(1) 국제기준

일반적으로 국제규범들이 요구하고 있는 개인정보보호기구(DPA)의 독립성은 인권기구와 같은 수준을 요구하고 있다. 1991년 UN 개인정보보호 가이드라인[96]은 "모든 회원국의 법은 자국의 국내법 체계에 따라 이상에서 열거한 원칙들의 준수를 감독할 책임기관을 지정하여야 한다. 그 기관은 공평성, 정보 처리 및 구축을 담당하는 개인 또는 기관에 대응한 독립성, 기술적인 능력을 갖추고 있어야 한다. 또한 이상의 원칙 이행을 명시하고 있는 국내법 조항을 위반한 경우 적합한 개인적 구제와 함께 처벌 또는 그 밖의 벌칙이 규정되어 있어야 한다."라고 하여 감독기구의 독립성을 추상적으로 강조하고 있다.

UN 개인정보보호 가이드라인이 추상적이라면, 세계개인정보감독기구회의(ICDPC)가 2002년에 채택한 ICDPC 가입 인증기준[97]은 보다 구체적이다. 감독기구가 개인정보보호기구(DPA)로 공인을 받기 위해서는 개인정보 및 프라이버시 보호 원칙과 실무에 있어서 최고의 전문기관이 되어야 하며. 광범위한

96) UN,「Guidelines for the regulation of computerized personal files」(1991) 제8조 참조.

97) 제23차 ICDPC, Criteria and Rules for Credentials Committee and the Accreditation Principles(2001, 2002년 개정)

활동영역에 걸쳐 개인정보 및 프라이버시를 보호·촉진할 명확한 권한과 보호업무 수행을 위해 필요한 모든 법적 권한을 가져야 한다. 구체적으로 동 인증기준은 평가항목을 ① 감독기구 설립의 법적근거, ② 감독기구의 자율성과 독립성, ③ 감독기구의 업무수행 기준·절차를 규정하고 있는 준거법과 국제기준의 일치여부, ④ 감독기구의 기능과 권한 등으로 나누어서 평가하고 있다.

먼저, 감독기구는 "원칙적으로" 법률에 의해서 설립되어야 하고, 해당 법률은 감독기구의 독립성과 기능수행에 필요한 능력을 뒷받침해야 하며, 개인정보보호 업무에만 전념할 것을 증명하여야 한다. 둘째, 감독기구의 구성원은 임기가 정해져 있어야 하고, 업무 수행능력 부재, 근무태만, 중대한 불법행위를 이유로만 해임될 수 있어야 한다. 셋째, 감독기구가 관리·감독의 기준으로 삼고 있는 준거법이 OECD 프라이버시 가이드라인, UN 가이드라인, EU 디렉티브 등과 부합해야 한다. 마지막으로 감독기구는 단순한 자문기구(advisory)이어서는 안 되며 법적 또는 행정적 조치를 취할 수 있는 감독권한을 가져야 한다. 최소한 법률준수(compliance), 감시·감독(supervision), 조사·검사(investigation), 피해구제(redress), 안내·지도(guidance), 교육·홍보(public education) 등의 기능을 수행하여야 한다.

(2) 유럽연합

2012년 EU Regulation[98]은 감독기구의 독립성 요건으로 ① 주어진 의무와 권한의 행사에 있어서 완전히 독립적으로 활동해야 하고, ② 감독기구의 구성원은 임무수행 중 누구로부터도 지시를 구하거나 받아서는 안 되며, ③ 보수의 유무를 불문하고 양립하기 어려운 직업을 겸직해서는 안 되며, 이해관계가 있는 사안에 대해서는 제척·기피·회피해야 하고, ④ 의무와 권한의 효과적 수행에 필요한 인력, 기술, 예산, 공간, 인프라 등의 제공이 보장되어 있어야 하며, ⑤ 감독기관이 임명하고 기관의 장의 지시에 따르는 고유의 직원을 보유할 권한이 보장되어야 하고, ⑥ 독립성에 영향을 미치지 않는 방법으로 예산 통제가 이루어져야 한다고 규정하고 있다.

동시에 감독기구의 구성원의 자격으로는 ① 의회 또는 관련 정부에 의하여 임명되어야 하며, ② 의심의 여지없이 독립적이고 임무수행에 요구되는 경험과 기술을 증명할 수 있어야 하며, ③ 중대한 비행이 있는 경우를 제외하고는 임기, 연금 등이 보장되어야 한다고 규정하고 있다.

98) 제46조 내지 제50조 참조.

(3) 일본・미국 등

일본과 미국은 별도의 독립된 개인정보보호 감독기구를 두고 있지 않다. 일본은 공공기관 즉 행정기관과 독립행정법인이 보유한 개인정보에 대해서는 총무성 장관이 감독기관의 역할을 수행하고, 민간부문에 대해서는 각 주무부처 장관이 소관분야에 대하여 감독기관으로서의 역할을 수행한다. 또한 민간부문에는 주무부처 장관이 신청을 받아 인정한 인정 개인정보보호 단체들이 있다. 그러나 이들 중 어느 것도 국제규범이 요구하고 있는 독립된 개인정보보호 감독기구로서의 요건을 구비하고 있지는 않다. 미국도 연방정부기관들의 개인정보처리에 대하여는 연방 프라이버시법(Privacy Act)에 따라 예산관리처(OMB, Office of Management and Budget)가 담당하지만, 민간부문의 개인정보처리에 대하여는 주로 연방 공정거래위원회(FTC, Federal Trade Commission)가 공정거래법 제5조에 따라 담당한다. 그러나 두 기관 모두 독립된 개인정보보호 감독기관은 아니다.

2012년 EU Regulation	일본 개인정보보호법
제46조(감독기관) 1. 회원국은 하나 이상의 공공기관이 개인정보의 처리와 관	제37조(인정) ①개인정보취급사업자의 개인정보의 적정한 취급의 확보를 목적으

련된 자연인의 기본권과 자유를 보호하고 유럽연합 내에서 개인정보의 자유로운 이동을 용이하게 하기 위해 이 법안의 적용을 감시하고 나아가 유럽연합 전체에 적용되는 것에 기여해야 하는 책임을 지도록 규정해야 한다. 이 같은 목적을 위하여 해당 공공기관들은 유럽집행위원회와 서로 협력하여야 한다. 2. 감독기관이 하나 이상인 경우 회원국은 유럽정보보호위원회(European Data Protection Board)에 효율적인 참여를 위해 연락창구(contact point)로서의 역할을 할 감독기구를 지정해야 하며 제57조에서 언급한 일관성 보장 장치와 관련된 규정을 다른 기관들이 준수하는 것을 보증할 수 있는 장치를 마련하여야 한다. 3. 각 회원국은 늦어도 제91조 (2)항에서 규정한 날까지 본 장(章)에 따라 채	로서 다음 각 호에 게재된 업무를 행하는 법인(법인이 아닌 단체의 대표자 또는 관리인이 있는 자를 포함한다. 다음 조 제3호에 있어서도 같다)은 주무장관의 인정을 받을 수 있다. 1. 업무의 대상이 되는 개인정보취급사업자(이하 「대상 사업자」라 한다)의 개인정보의 취급에 관한 제42조의 규정에 의한 고충의 처리 2. 개인정보의 적정한 취급의 확보에 기여하는 사항에 관한 대상 사업자에 대한 정보 제공 3. 전 2호에 게재한 사항 이외에 대상 사업자의 개인정보의 적정한 취급의 확보에 관하여 필요한 업무 ② 전항의 인정을 받으려 하는 자는 정령에서 정하는 바에 의하여 주무장관에게 신청하여야 한다. ③ 주무장관은 제1항의 인정을 한 때에는 그 취지를

택한 법률의 규정과 이후의 법률의 수정사항을 집행위원회에 알려야 한다.	공시하여야 한다.
제47조(독립성) 1. 감독기관은 부여받은 의무를 이행하고 권한을 행사함에 있어서 완전히 독립적이어야 한다. 2. 감독기관의 구성원은 자신의 의무를 이행함에 있어서 다른 사람으로부터 지시를 구하거나 받아서는 안 된다. 3. 감독기관의 구성원은 자신의 임무와 일치하지 않는 행동을 해서는 안 되며, 영리 유무를 떠나 임기 중 임무와 일치하지 않는 직업을 가져서는 안 된다. 4. 감독기관의 구성원은 임기가 끝난 후에도 어떤 직책에 대한 임명을 수락하거나 이익을 받음에 있어서 신중하고도 성실하게 행동하여야 한다. 5. 회원국은 감독기관이 자신의 의무와 권한을 효과적으로 이행하기 위해 필	제38조(결격조항) 다음 각 호의 1에 해당하는 자는 전조 제1항의 인정을 받을 수 없다. 1. 이 법률의 규정에 의한 형의 선고를 받고 그 집행이 끝나거나 또는 집행을 받지 않게 된 날로부터 2년이 경과되지 아니한 자 2. 제48조제1항의 규정에 의한 인정이 취소되고 그 취소된 날로부터 2년이 경과되지 아니한 자 3. 그 업무를 행하는 임원(법인이 아닌 단체에서는 단체의 대표자 또는 관리인을 포함한다. 이하 이조에 있어서 같다) 중에서 다음의 1에 해당하는 자가 있는 경우 가. 금고 이상의 형에 처해지거나 또는 이 법률의 규정에 의한 형의 선고를 받고 그 집행이 끝나거나 또는 집행을 받지 않게

요한 적절한 인력, 기술 및 예산, 시설, 기반 등과 함께, 유럽정보보호위원회에서의 상호 지원, 협력, 참여 등에 필요한 것들을 제공받을 수 있도록 보장하여야 한다. 6. 회원국은 감독기관에 의해서 임명도고 감독기관의 장의 지휘를 받는 직원을 자체적으로 고용하는 것을 보장하여야 한다. 7. 회원국은 감독기관이 독립성에 영향을 받지 않는 방법으로 예산통제를 받도록 해야 하고, 연도별 분리 예산을 갖도록 해야 한다. 또한, 예산은 공개되어야 한다.	된 날로부터 2년이 경과되지 아니한 자 나. 제48조제1항의 규정에 의한 인정이 취소된 법인의 경우 그 취소일 전 30일 이내에 그 임원이었던 자로서 그 취소일로부터 2년이 경과되지 아니한 자
제48조(감독기관 구성원의 자격) 1. 회원국은 감독기관의 구성원들이 의회나 관련정부기관에 의해 임명되도록 규정해야 한다. 2. 구성원은 의심할 여지없이 독립성을 갖추고 개인정보보호 분야에서 자신의 의무를 이행하는데 필요한	

경험과 자질을 갖추고 있다는 것이 증명된 사람들 중에서 임명되어야 한다. 3. 구성원의 임무는 제5항에 따른 임기의 만료, 사의, 강제퇴직의 경우에 종료되어야 한다. 4. 구성원이 임무수행에 필요한 자격을 충족하지 못하거나 심각한 위법행위를 한 것으로 판단되는 경우 해당 구성원은 법원에 의하여 연금 등의 혜택을 받을 수 있는 권리를 박탈당할 수 있다. 5. 임기가 만료되거나 구성원이 사임하는 경우, 해당 구성원은 새로운 구성원이 임명될 때까지 의무를 계속 이행해야 한다.	
제49조(감독기관의 설립에 과한 원칙) 회원국은 이 법안의 범위 내에서 회원국의 법률로 다음 각 호의 사항을 규정하여야 한다. (a) 감독기관의 설립 및 지위;	제39조(인정의 기준) 주무장관은 제37조제1항의 인정신청이 다음 각 호의 1이라도 충족하지 못한다고 인정한 경우에는 그 인정을 하여서는 아니 된다. 1. 제37조제1항 각 호에 게

(b) 구성원의 임무 이행에 필요한 자질, 경험, 기술; (c) 구성원의 임명을 위한 규정 및 절차와 임무에 배치되는 행동 및 직업에 대한 규정; (d) 구성원의 임기는 4년 이상으로 할 것. 다만, 시차를 둔 임명 절차를 통해 감독기관의 독립성을 보호하는데 필요한 경우, 이 법안이 시행된 후 첫 번째 임명의 경우에는 4년 이하일 수 있다; (e) 구성원이 재임용될 수 있는지 여부; (f) 구성원 및 직원의 임무와 관련된 규정 및 일반 조건; (g) 구성원이 임무 이행에 필요한 조건을 더 이상 충족하지 못하는 경우 및 심각한 위법행위를 한 경우를 포함하여 구성원의 임무 종료에 대한 규정 및 절차;	재된 업무를 적정하고 확실하게 행함에 필요한 업무의 실시 방법이 정하여져 있을 것 2. 제37조제1항 각 호에 게재된 업무를 적정하고 확실하게 행함에 충분한 지식 또는 능력과 경리적 기초를 가지고 있을 것 3. 제37조제1항 각 호에 게재된 업무 이외의 업무를 행하고 있는 경우에는 그 업무를 행함에 의해 동항 각 호에 게재된 업무가 불공정하게 될 우려가 없을 것
제50조(직무상 비밀 유지) 구성원 및 직원은 임기 중	

또는 임기 이후에도 임무 수행 중 알게 된 비밀정보에 대해 비밀을 유지하여야 한다.	

제2절 보호위원회의 역할 재정립 : 집행체계의 통일

1. 현황 및 문제점

우리나라는 일반법으로써 개인정보보호법이 제정되어 있음에도 불구하고 개인정보 보호업무가 각 부처에 분산되어 있어 중복규제와 차별규제가 여전히 반복되고 있다. 보호위원회, 행정안전부, 방송통신위원회, 금융위원회 등이 각자 소관 법률에 따라 개인정보 보호행정을 펼치고 있고, 이들 기관을 지원·보조하는 기관도 분산되어 있어 한국인터넷진흥원(KISA), 국가정보화진흥원(NIA), 금융감독원 등 다양하다.

그 결과 개인정보보호 관련법령의 해석이 각기 다르고, 동일한 사항에 대하여 여러 부처의 조사와 관리·감독을 받아야 하며, 규제당국마다 규제수준에 있어서도 차이가 크고, 무엇보다 복잡한 법률체계와 집행체계로 인해 법집행에 대한 예측가능성이 현저히 떨어져 수범자인 기업들이 법을 준수하기 어려

우며, 법을 준수하기 위해서는 과도한 컴플라이언스 비용을 지불해야 한다.

현행 개인정보보호법의 집행체계는 수범자인 기업들뿐만 아니라 규제당국에 있어서도 예산 및 인력 낭비가 적지 않다. 보호위원회, 행정안전부, 방송통신위원회, 금융위원회 등 정부기관과 한국인터넷진흥원(KISA), 국가정보화진흥원(NIA), 금융감독원 등 정부기관을 지원하는 기관들이 개인정보보호 업무에 투입하는 인력은 약 170여명에 이르고 있어 어느 선진국의 개인정보보호 감독기구와 비교해서도 규모면에서 결코 뒤지지 않고 있다. 일반적으로 선진국 개인정보보로 감독기구의 인력이 30~200명 수준임[99]을 고려한다면 적은 인력이라고 할 수 없다.

규제기관별 개인정보관련 인력 현황

합계	개보위	행안부	방통위	금융위	KISA	NIA	금감원
관련 법률	개보법	개보법	망법·위치법	신용정보법	개보법/망법/위치법	개보법	신용정보법
170명	30명	60명	10명	5명	45명	20명	5명

99) 영국 : 200명, 프랑스 : 200명, 독일(연방) : 70명, 스웨덴 : 40명, 캐나다(연방) : 100명, 호주(연방) : 40명, 뉴질랜드 : 32명, 홍콩 : 34명. 영국, 프랑스 등은 개인정보보호 감독기구가 개인정보보호업무 이외에 정보공개업무 등도 맡고 있다.

이와 같은 현상은 개인정보보호법이 독립된 개인정보보호 감독기구로 개인정보보호위원회를 설립해 놓기는 하였지만, 보호위원회에게 그 위상에 맞는 역할과 기능을 부여하고 있지 않기 때문이라고 할 수 있다.

2. 개정방향

정보통신망법, 위치정보법, 신용정보법 등이 존속하고 있고, 각 부처마다 소관분야에 대한 관할권을 강력하게 주장하고 있는 현실에서 개인정보 보호 행정체계의 대변화는 쉽지 않을 것으로 생각된다. 따라서 이하에서는 보호위원회의 역할 재정립을 중심으로 개인정보보호법의 집행체계에 대한 개선안을 제시한다.

(1안) 대통합안 : 개인정보정책을 모두 보호위원회로 일원화하는 방안

개인정보보호정책을 효율적으로 추진하고 일관성 있는 법집행을 위해서는 모든 개인정보보호관련 정책을 독립기구인 보호위원회로 통합하는 것이 바람직하다. 이 방법은 이미 유럽연

합 회원국들이 20년 이상 채택해 온 것으로 검증된 방법이라고 할 수 있다. 유럽연합은 모든 개인정보보호 관련 법률 이슈가 개인정보보호법으로 통합되어 있고, 법집행도 개인정보감독기구로 통일되어 있다.

모든 개인정보보호정책을 보호위원회로 통합하기 위해서는 정보통신망법, 위치정보법, 신용정보법 등 개별법도 폐지하고 개인정보보호법 체계 내로 흡수되어야 한다. 그러나 다른 법률의 폐지는 이 연구과제의 범위를 초과하는 것이므로, 여기서는 개인정보보호법 내에서 주로 행정안전부장관의 권한을 보호위원회로 통합하는 것에 대해서만 검토한다. 1안을 채택할 경우 개인정보보호법은 사실상 전문개정을 해야 하므로 여기서는 개정안에 대한 신구 조문대비표는 만들지 않고 통합대상이 되는 행정안전부장관의 권한에 대해서만 정리하는 것으로 하였다.

1안에 대해서는 보호위원회가 명분상으로는 물론 실질적으로 사실상 독립된 행정규제위원회가 되어 “작은 정부” 추세에 어긋난다거나 위원회 제도의 특성상 독임제 행정기관에 비해서 효율성과 집행력이 떨어질 수 있다는 비판이 있을 수 있다. 또, 소규모의 보호위위원회가 행정안전부, 법무부, 복지부, 교육부, 경찰청 등과 같이 막대한 권한을 가진 거대 행정기관을 상대로 업무를 감당할 수 있는 능력이 있는지에 대해서도 논란이 생길 수 있다.

통합대상인 행정안전부장관의 권한

관련조문	통합대상 내용
제9조	개인정보 보호 기본계획
제11조	기본계획 수립·추진을 위한 자료제출 등 요구
제12조	표준 개인정보 보호지침 제정
제13조	자율규제의 촉진 및 지원
제24조	주민등록번호 대체수단 제공 방법 지원
제30조	개인정보 처리방침의 작성지침 작성·권장
제32조	개인정보파일 등록 및 공개
제33조	개인정보영향평가 결과에 대한 의견제출
제34조	개인정보 유출 신고접수
제40조	개인정보 분쟁조정위원회의 설치 및 구성
제61조	의견제시 및 개선권고(법령·조례, 처리실태 개선)
제62조	침해사실 신고 등 접수(침해신고센터 운영)
제63조	자료제출 요구 및 검사
제64조	민간부문의 법위반에 대한 시정조치 명령
제65조	고발 및 징계권고
제66조	시정명령, 징계권고 등 결과의 공표
제68조	권한의 위임·위탁
제75조	과태료의 징수 및 부과

(2안) 부분통합안 : 행정안전부장관의 권한 중 일부를 보호위원회로 이전하는 방안

현행 개인정보 보호체계는 중복규제에 따른 어려움이 많고 고비용적이지만, 현행 시스템을 유지하면서 행정안전부장관의 권한 중에서 총괄·조정기능에 해당하는 것은 보호위원회로 이전하고, 행정안전부장관은 순수한 집행기능만 수행하도록 하는 방안이다. 상기 행정안전부장관의 권한 중에서 개인정보 보호 기본계획 수립 및 점검(제9조 및 제11조), 표준 개인정보 보호지침의 제정·권고(제12조), 개인정보유출 신고접수(제34조), 개인정보 분쟁조정위원회의 설치 및 구성(제40조), 침해사실 신고 등 접수(침해신고센터 운영)(제62조) 등은 총괄·조정적 성격이 강하다고 할 수 있다.

또한 보호위원회는 개인정보보호 감독기구로서 행정안전부장관이나 관계중앙행정기관의 장이 개선권고나 시정명령을 게을리 하거나 불충분하게 한 경우 “보충적으로” 개인정보처리자에게 의견제시 및 개선권고(제61조), 법위반에 대한 시정조치 명령(민간부문)(제64조) 등도 할 수 있어야 한다. 끝으로 보호위원회는 대통령 소속이라서 법리상 논란이 있을 수 있으나 소관 사무에 관하여 국무총리에게 의안(개인정보보호법의 시행에 관한 대통령령 안을 포함한다) 제출을 건의할 수 있도록

하는 것이 바람직하다.

2안에 대해서는 기존의 중복규제와 집행체계 혼선에 대해서는 아무런 개선책이 없이 부처 간에 나눠 먹기식으로 권한만 재배치했다는 비판을 받을 수 있고, 특히 기존의 행정안전부장관의 독자 권한으로 되어 있던 개인정보처리자에 대한 의견제시 및 개선 권고권(제61조)과 법위반에 대한 시정조치 명령권(민간부문)(제64조)을 보호위원회에게도 부여함으로써 중복규제를 더욱 심화시키고 있다는 비판이 있을 수 있다. 제61조 및 제64조의 개정안에 대해서는 다음 항에서 별도로 설명한다.

행정안전부에서 보호위원회로의 이전 권한

관련조문	통합대상 내용	비고
제9조	개인정보 보호 기본계획	이전
제11조	기본계획 수립·추진을 위한 자료제출 등 요구	이전
제12조	표준 개인정보 보호지침 제정	이전
제34조	개인정보 유출 신고접수	이전
제40조	개인정보 분쟁조정위원회의 설치 및 구성	이전
제61조	의견제시 및 개선권고(법령·조례, 처리실태 개선)	공동
제62조	침해사실 신고 등 접수(침해신고센터 운영)	이전
제64조	민간부문의 법위반에 대한 시정조치 명령	공동

3. 외국사례

개인정보보호를 위한 집행체계는 크게 세 가지 유형으로 나뉜다. 유럽연합 회원국들과 같이 개인정보보호 감독기구가 공공과 민간 부문을 구분하지 않고 모든 영역을 통일해서 집행하는 유럽형(통합형)과 각 중앙행정기관이 소관 부처별로 나눠서 집행하는 일본형(분산형) 그리고 공공부문과 민간부문으로 나누어 공공부문은 관리예산처(OMB)가 담당하고 민간부문은 연방거래위원회(FTC)가 담당하는 미국형(중도형)으로 나눌 수 있다. 우리나라는 유럽형과 일본형이 뒤섞인 혼합형이라고 할 수 있다.

우선 유럽연합은 개인정보처리와 관련한 모든 권한과 의무가 개인정보보호 감독기구에 집중되어 있다. 이에 따라 유럽연합 회원국의 개인정보 감독기구들은 개인정보보호 정책과 행정을 전담해서 처리한다. 즉 EU에서는 개인정보 보호업무가 소관 분야에 따라 부처별로 나뉘어 있거나 기능적으로 분산되어 있지 않고 감독기구에 집중되어 있다. 또한 통일적인 법 집행원칙에 따라 개별법에 의한 개인정보처리에 대해서도 원칙적으로 감독기구가 관장한다. 따라서 중복규제나 규제혼선은 나타나지 않는다.

이에 따라 유럽연합 개인정보보호 감독기구들의 업무는 상담·자문에서 진정처리, 시정명령, 행정제재 등에 이르기까지

전방에 걸치며, 주요 업무는 ① 법령 준수 여부 모니터링, ② 진정사건의 접수 및 조사, ③ 다른 감독기구들과의 상호 협력 및 정보 공유, ④ 직권, 진정 등에 조사 및 결과 통지, ⑤ 개인정보에 영향을 미치는 기술발전 등의 모니터링, ⑥ 정보주체의 권리와 자유에 특별한 위험을 야기하는 개인정보처리에 대한 사전승인, ⑦ 행동규약(codes of conducts)에 대한 의견제시, ⑨ BCR(binding corporate rules)에 대한 승인, ⑩ 대중, 특히 어린이들에 대한 개인정보보호 인식제고, ⑪ 정보주체의 권리 행사에 대한 상담·자문, ⑫ 불만처리신청 양식의 제공, ⑬ 연차보고서의 작성 및 의회 보고, 대중 공개 등이다.[100]

이와 달리 일본은 개인정보보호 업무 전담기관이 없이 소관 분야와 기능별로 개인정보보호 관련 업무가 분산되어 있다. 민간부문에 대하여는 분야별로 주무부장관과 지방자치단체가 개인정보 보호업무를 수행하고(제32조 내지 제36조), 행정기관과 독립행정법인에 대하여는 총무성장관이 개인정보보호기구로서 업무를 수행한다.[101] 또한 관계 성·청에는 주무부장관의 인정을 받아 설치된 인정 개인정보보호단체들이 있는데 이들은 비록 민간단체이지만 정보주체가 신청한 개인정보 고충처리, 개인정보처리자에 대한 정보제공, 그밖에 개인정보의 적정한 취급을 확보하기 위한 사업을 추진한다(제37조 내지 제49조).

---

100) 2012년 EU Regulation 제52조 참조.

101) 행정기관이 보유하는 개인정보의 보호에 관한 법률(2003년) 제49조 내지 제51조. 독립행정법인이 보유하는 개인정보의 보호에 관한 법률(2003년) 제49조 내지 제51조.

공공부문과 민간부문 전체를 총괄하는 기능은 내각총리대신이 수행한다. 내각총리대신은 개인정보보호에 관한 시책의 종합적이고 일체적인 추진을 위하여 개인정보보호에 관한 기본방침을 수립해야 하며, 「국민생활심의회」의 의견을 거쳐 각의로써 결정해 공표·시행한다(제32조 내지 제37조). 또 내각총리대신은 관계 행정기관 및 내각의 관할 아래 있는 기관, 내각부, 궁내부 등에 대하여 개인정보보호법의 시행상황에 관한 보고를 요구할 수 있고 매년 그 보고결과를 취합하여 개요를 공표할 수 있다(제53조).

그 밖에 공공기관의 개인정보처리와 관련하여 정보주체의 권리구제 업무를 담당하는 기구로 정보공개·개인정보보호심사회가 있다. 행정기관이나 독립행정법인의 열람거절, 정정거절, 이용정지거절 등의 결정에 대하여 불복이 있는 자는 행정불복심사법에 따라 이의제기를 할 수 있는데, 이 경우 해당 불복신청에 대한 재결 또는 결정을 해야 하는 행정기관의 장 또는 독립행정법인은 정보공개·개인정보보호심사회[102]에 자문을

102) 정보공개·개인정보보호심사회는 15인의 위원(5명 이내의 상근위원)구성되며, 위원은 양원의 동의를 얻어 내각총리대신이 임명한다. 심사회의 사무를 처리하기 위하여 심사회에 사무국을 두며, 심사회는 해당 공공기관에 대하여 필요하다고 인정하는 경우 행정문서, 보유개인정보 등을 열람, 제출 등을 요구하거나 조사할 수 있으며, 이 경우 해당 공공기관은 심사회의 요구를 거절할 수 없다. 또한 심사회는 불복신청인, 참가인, 공공기관 등에게 의견서 또는 자료의 제출을 요구하거나 알고 있는 사실을 진술하게 하거나, 감정을 요구하는 등의 조치를 할 수 있다(정보

구해야 한다.[103]

미국은 개인정보보호를 위한 별도의 전담기구는 없다. 다만, 공공부문과 민간부문에서 예산관리처(OMB)와 연방거래위원회(FTC)가 각각 개인정보보호기구로서의 역할을 담당하고 있다. 공공부문에 있어서는 예산관리처[104]가 「1974년 프라이버시법」에 따라 연방정부의 프라이버시 또는 개인정보보호 정책을 정립하는 역할을 맡고 있다. 그러나 예산관리처는 우리나라의 기획재정부와 같이 예산편성과 운용 등 국가재정운영 전반에 관한 정책을 수립하고 집행하는 역할을 하는 기구인 바, 프라이버시 보호와 관련하여서도 예산관리차원에서만 제한적인 역할을 맡고 있다. 한편 민간부문에 있어서는 연방거래위원회가 아동의 온라인 프라이버시, 소비자신용정보, 비디오프라이버시, 공정한 거래관행과 관련한 프라이버시 등을 보호하는 법

공개・개인정보보호심사회 설치법, 2003년).

103) 행정기관이 보유하는 개인정보의 보호에 관한 법률(2003년) 제42조 내지 제44조. 독립행정법인이 보유하는 개인정보의 보호에 관한 법률(2003년) 제42조 내지 제44조.

104) 예산관리처는 1921년 창설된 예산처(BOB : Bureau of Budget)를 1970년 재정비한 기구로서 대통령의 예산집행 및 관리, 기타 정책의 수립 및 시행을 지원한다. 1999년에는 연방정부기관의 프라이버시에 대한 접근태도를 조화시키고자 예산관리국 내 최고 프라이버시 자문역(Chief Counselor for Privacy)이 임명되기도 하였는데, 이는 단순한 자문기능을 하는 제한적인 권한만 가지고 있었다. 그러나 부시 행정부가 들어서면서는 프라이버시 자문역 제도는 폐지되었다. (EPIC & PI, supra note 138, http://www.privacyinternational.org/survey/phr2003/countries/unitedstates.htm)

률을 집행하고 준수여부를 감독할 권한을 부여받아 행사하고 있다.

그러나 미국에서도 우리나라와 마찬가지로 분야별로 다수의 연방 개별법들이 난무하고, 주별로도 다수의 개별법이 제정되고 있어 기업들에게 많은 혼란을 주고 있다. 이에 따라 개인정보보호에 관한 연방 일반법을 제정해서 개인정보처리에 관한 원칙을 통일하고, 그 법률의 집행권한을 연방거래위원회에 부여하고자 하는 시도가 백악관과 FTC를 중심으로 해서 계속 시도되고 있다.[105]

2012년 EU Regulation	일본 개인정보보호법
제52조(임무) 1. 감독기관은 (a) 이 법안의 적용을 감시하고 보증해야 한다. (b) 제73조에 따라 정보주체 또는 정보주체를 대표하는 협회가 제기하는 불만사항을 들어야 하고, 적절한 범위 내에서 문제를 조사하고, 정보주체나 협회	제36조(주무장관) ①이 절의 규정에서 주무장관은 다음과 같다. 다만, 내각총리대신은 이 절의 규정의 원활한 실시를 위하여 필요하다고 인정되는 경우에는 개인정보취급사업자가 행하는 개인정보의 취급 중

105) The White House, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, February 23, 2012 참조.

에 적절한 기간 내에-특히 조사가 더 필요하거나 다른 감독기관과의 협력이 필요한 경우-불만사항의 진행 및 처리 결과에 대해 알려야 한다. (c) 다른 감독기관과 정보를 공유하고 상호 지원을 제공하며, 이 법안 규정의 일관성 있는 적용 및 시행을 보증해야 한다. (d) 자발적으로 또는 불만사항에 기초하여 또는 다른 감독기관의 요청에 따라 조사를 하고, 정보주체가 감독기관에게 불만사항을 제기한 경우에는 정보주체에게 적절한 기간 내에 조사 결과를 알려야 한다. (e) 개인정보 보호에 영향을 미치는 경우 적절한 개발 특히 정보, 통신기술, 상업적 관행 등의 개발을 감독해야 한다. (f) 개인정보 처리와 연관된 개인의 권리 및 자유와 관련하여 회원국 입법 및	특정한 사항에 관하여 특정한 장관 또는 국가공안위원회(이하 「장관 등」이라 한다)를 주무장관으로 지정할 수 있다. 1. 개인정보취급사업자가 행하는 개인정보의 취급 중 고용관리에 관한 사항에 관해서는, 후생노동장관(선원의 고용관리에 관한 사항에 관해서는 국토교통장관) 및 당해 개인정보취급사업자가 행하는 사업을 소관하는 장관 등 2. 개인정보취급사업자가 행하는 개인정보의 취급 중 전호에 게재된 사항 이외의 사항에 관해서는 당해 개인정보취급사업자가 행하는 사업을 소관하는 장관 등 ②내각총리대신은 전항단서의 규정에 의한 주무장관을 지정하는 때에는 그 취지를 공시하여야 한다.

행정기관의 자문을 받아야 한다. (g) 제34조에서 언급한 처리를 승인하고 이와 관련된 자문을 받아야 한다. (h) 제38조 (2)항에 따른 윤리규범 초안에 대한 의견을 제시해야 한다. (i) 제43조에 따른 구속력 있는 기업규칙을 승인해야 한다. (j) 유럽정보보호위원회의 활동에 참여해야 한다. 2. 각 감독기관은 개인정보 처리와 관련하여 위험에 처한 대중의 인식, 규정, 안정 장치, 권리 등을 장려해야 한다. 3. 감독기관은 정보주체의 권리 행사와 관련하여 조언을 해야 하며, 필요한 경우 이를 위해 다른 회원국 감독기관과 협력해야 한다. 4. 제1항의 (b)에서 언급한 불만사항과 관련하여, 감독기관은 다른 통신수단을 배제하지 않으면서 전자적으로 작성할 수 있는 불만	③각 주무장관은 이 절의 규정의 시행에 있어서 상호 긴밀히 연락하고 또 협력하여야 한다.

사항 제출 형식을 제공해야 한다. 5. 감독기관의 의무 이행에 대해 정보주체는 비용을 부담하지 않는다. 6. 요청이 명백히 과도한 경우, 특히 반복으로 인해 과도한 경우, 감독기관은 정보주체가 요청한 행동에 대해 수수료를 부과하거나 요청 행동을 취하지 않을 수 있다. 감독기관은 요청이 명백히 과도하다는 것을 입증할 책임을 부담해야 한다.	
제73조(감독기관에 대한 불만 제기권리) 1. 다른 어떠한 행정적 또는 사법적 구제조치(remedy)를 침해함이 없이 모든 정보주체는 자신과 관련된 개인정보의 처리가 이 법안을 준수하지 않는다고 판단되는 경우, 아무 회원국의 감독기관에 불만을 제기할 수 있는 권리를 갖고 있다. 2. 개인정보 보호와 관련된 정보주체의 권리와 이익을	

보호한다는 목적을 가진 그리고 회원국 법률에 따라 적절하게 구성된 기관, 단체, 협회는 이 법안에 따른 정보주체의 권리가 개인정보 처리 결과로 인해 침해 받았다고 판단되는 경우 하나 이상의 정보주체를 대신하여 아무 회원국의 감독기관에 불만을 제기할 수 있는 권리를 갖고 있다. 3. 정보주체의 불만과는 별도로 2항에서 언급한 단체, 기관, 협회는 개인정보의 침해가 발생하였다고 판단되는 경우, 아무 회원국 감독기관에 불만을 제기할 수 있는 권리를 갖고 있다.	

제3절 보호위원회의 조사권 등 권한 강화 (제8조)

1. 현황 및 문제점

개인정보보호법상 보호위원회는 독립된 감독기구로서의 역할을 부여받고 있으나 그 역할을 수행할 수 있는 권한은 충분하지 못하다. 보호위원회는 심의·의결을 위하여 필요하면 관계 공무원, 개인정보 보호에 관한 전문 지식이 있는 사람이나 시민사회단체 및 관련 사업자로부터 의견을 들을 수 있고, 관계 기관 등에 대하여 자료 등의 제출을 요구할 수 있으나, 현장에 출입하여 업무상황, 장부, 서류 등을 검사하거나 조사할 수 있는 권한은 없다.

또한, 보호위원회는 심의·의결을 주요 기능으로 하고 있으나 심의·의결의 법적 성격이 분명하지 아니하여 심의·의결 결과에 대한 법적 구속력에 대해서 논란이 있을 수 있다. 극단적인 경우 보호위원회의 심의·의결 결과를 무시하거나 거부하는 경우도 있을 수 있다. 그러나 현행 규정상으로는 심의·의결을 구속력도 불분명하고 강제할 수 있는 제도적 장치도 마련되어 있지 않다.

2. 개정방향

보호위원회가 개인정보침해 가능성이 있거나 개인정보보호에 영향을 미칠 수 있는 법령에 대하여 충분히 필터링 기능을 수행할 수 있도록 중앙행정기관의 장 또는 지방자치단체의 장이 개인정보 및 사생활에 영향을 미치는 내용을 포함하고 있는 법령을 제정하거나 개정하려는 경우 미리 보호위원회에 통지하도록 하고, 국회는 개인정보 및 사생활에 영향을 미치는 내용의 의안에 대하여 보호위원회에 의견을 요청할 수 있게 하는 것이 바람직하다.

또한, 보호위원회가 심의·의결을 충실하게 할 수 있도록 기존에 인정하고 있던 의견 청취권과 자료 등의 제출요구권 외에 사실조회 요구권과 현장 조사·검사권을 부여하여야 한다. 비록 대부분의 심의·의결 사항이 의견청취권과 자료 등의 제출 요구권으로 충분하다고 하더라도 향후 개인정보보호 이슈가 증가하고 정보주체들의 권리의식이 향상됨에 따라 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 심의안건이 늘어날 수 있고, 그런 경우에는 개인정보의 처리 상황이나 관행을 분석·확인하기 위해 현장 조사·검사가 요구될 있다. 특히 상대방이 민간 기업이라면 자료 등의 제출 요구권만으로는 충분하지 못한 경우가 많이 발생할 것이다.

심의·의결 결과에 대한 법적 효력도 이를 명확히 할 필요가

있다. 사실 제8조제1항에서 규정하고 있는 대부분의 심의·의결 사항이 명시적으로 법적 구속력을 인정하기도 애매하고, 그렇다고 보호위원회의 심의·의결 결과를 무시하거나 거부해도 좋다는 것은 더더욱 아니다. 따라서 관계 기관 또는 개인정보처리자는 특별한 사유가 없는 한 보호위원회의 심의·의결 결과를 따르도록 하되, 심의·의결 결과에 불복이 있는 자에게는 서면으로 그 사유를 밝히고 재의를 요구할 수 있게 하는 것이 오히려 보호위원회 심의·의결 결과의 수용력을 높이고 보호위원회의 신뢰성과 위상을 향상시키는 데도 기여할 것이다.

아울러, 보호위원회가 심의·의결을 한 경우에는 그 결과를 언론 등을 통해 널리 공표하게 함으로써 보호위원회의 활동 결과를 정보주체들에게 알릴 수 있고, 동시에 기업 등 개인정보처리자에 대하여는 보호위원회의 결정에 대하여 전사 차원의 관심을 갖게 할 수 있을 것으로 기대된다. 그러나 모든 심의·의결 결과를 공표하게 할 경우 예상치 못한 피해가 있을 수 있으므로 제8조 제1항 제6호와 같이 그 결과를 공표하면 해킹에 악용될 우려가 있거나, 제8조 제1항 제11호와 같이 예측하기 어려운 사안에 대해서는 보호위원회의 결정으로 공표하지 아니할 수 있게 하였다.

예컨대 제33조제3항에 따른 영향평가 결과를 공표할 경우 해당 공공기관 개인정보처리시스템이나 유사한 시스템을 도입하고 있는 기관의 보안상 취약점이 공개되어 해킹의 대상이 될

수 있다. 또 제8조 제1항 제11호는 심의·의결대상을 특별히 제한하고 있지 아니한 바, 정부의 비밀업무나 외교상 업무가 심의·의결의 대상이 될 수도 있고 특정 민간기업의 신기술에 대한 사항도 포함될 수 있으므로 모든 심의·의결 결과를 무조건 공개하게 하는 것은 부작용을 동반할 수 있다.

개정안 신·구 대조표

현 행	개 정 안
제8조(보호위원회의 기능 등) ① 보호위원회는 다음 각 호의 사항을 심의·의결한다. 1. 제9조에 따른 기본계획 및 제10조에 따른 시행계획 2. 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항 3. 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항 4. 개인정보 보호에 관한 법령의 해석·운용에 관한 사항 5. 제18조제2항 제5호에 따	제8조(보호위원회의 기능 등) ① 보호위원회는 다음 각 호의 사항을 심의·의결한다. 1. 제9조에 따른 기본계획 및 제10조에 따른 시행계획 2. 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항 3. 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항 4. 개인정보 보호에 관한 법령의 해석·운용에 관한 사항 5. 제18조제2항 제5호에 따

른 개인정보의 이용·제공에 관한 사항 6. 제33조제3항에 따른 영향평가 결과에 관한 사항 7. 제61조제1항에 따른 의견제시에 관한 사항 8. 제64조제4항에 따른 조치의 권고에 관한 사항 9. 제66조에 따른 처리 결과의 공표에 관한 사항 10. 제67조제1항에 따른 연차보고서의 작성·제출에 관한 사항 11. 개인정보 보호와 관련하여 대통령, 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항 12. 그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의·의결하는 사항 <신 설>	른 개인정보의 이용·제공에 관한 사항 6. 제33조제3항에 따른 영향평가 결과에 관한 사항 7. 제61조제1항에 따른 의견제시에 관한 사항 8. 제64조제4항에 따른 조치의 권고에 관한 사항 9. 제66조에 따른 처리 결과의 공표에 관한 사항 10. 제67조제1항에 따른 연차보고서의 작성·제출에 관한 사항 11. 개인정보 보호와 관련하여 대통령, 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항 13. 그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의·의결하는 사항 ② 중앙행정기관의 장 또는 지방자치단체의 장은 개인정보 및 사생활에 영향을 미치는 내용을 포함하고 있는 법령을 제정하거나 개정하려는 경우 미리 보호위원회에 통지하여

	야 한다. 국회는 개인정보 및 사생활에 영향을 미치는 내용의 의안에 대하여 보호위원회에 의견을 요청할 수 있다.
② 보호위원회는 제1항 각 호의 사항을 심의·의결하기 위하여 필요하면 관계 공무원, 개인정보 보호에 관한 전문 지식이 있는 사람이나 시민사회단체 및 관련 사업자로부터 의견을 들을 수 있고, 관계 기관 등에 대하여 자료 등의 제출을 요구할 수 있다.	③ 보호위원회는 제1항 각 호의 사항을 심의·의결하기 위하여 필요하면 관계 공무원, 시민사회단체, 사업자 및 사업자단체, 관련 전문가 등으로부터 의견을 들을 수 있고, 관계 기관, 개인정보처리자 등에 대하여 자료 등의 제출이나 사실 조회를 요구할 수 있으며, 소속 공무원으로 하여금 개인정보처리자의 사무소나 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 조사·검사하게 할 수 있다.
<신 설>	④ 제2항에 따른 요구를 받은 기관 또는 개인은 지체 없이 협조하여야 한다.
<신 설>	⑤ 관계 기관 또는 개인정보처리자는 특별한 사유가 없는 한 제1항에 따른 보호위원회의 심의·의결 결

<신 설>	과를 따라야 한다. 보호위원회의 심의·의결 결과에 불복이 있는 자는 서면으로 그 사유를 밝히고 재의를 요구할 수 있다. ⑥ 보호위원회는 제1항의 심의·의결 결과를 공표하여야 한다. 다만, 제1항 제6호 및 제11호에 해당하는 사항에 대하여는 보호위원회의 결정으로 공표하지 아니할 수 있다.

3. 외국사례

개인정보보호 감독기구는 개인정보 침해를 예방하고 개인정보의 활용 환경을 개선하는 등 다양한 업무를 수행하여야 하기 때문에 일반적으로 여러 가지 권한이 부여되고 있다.

예컨대 2012년 EU Regulation은 개인정보 감독기구에 대하여 ① 법위반 사실 고지권 및 구제 명령권, ② 법령준수(정보주체의 자기결정권 보장 등) 명령, ③ 정보 및 자료 제출요청권, ④ 특별한 위험을 야기하는 개인정보처리에 대한 사전 승인 또는 자문 강제, ⑤ 개인정보처리자에 대한 경고권, ⑥ 법에

위반하여 처리된 개인정보의 파기, 삭제 등 명령 및 해당 정보를 제공받은 자에 대한 고지 명령, ⑦ 개인정보처리의 임시 또는 영구적 금지, ⑧ 제3국으로의 개인정보 제공에 대한 연기명령, ⑨ 개인정보보호 관련 이슈에 대한 의견 제시권, ⑩ 개인정보보호 관련 이슈에 대해 국민, 의회, 정부 등에 대한 정보제공, ⑪ 업무수행에 필요한 자료 및 개인정보에 대한 접근권, 현장방문권 등 조사권, ⑫ 사법 당국에 대한 고발권 및 법률절차 참가권, ⑬ 행정제재 부과권 등을 부여하고 있고,[106] 경고, 과징금 등 행정 제재권한을 부여하고 있다.[107]

그러나 독립된 개인정보보호 감독기관 없이 소관분야의 주무부장관이 개인정보 보호업무를 맡고 있는 일본의 경우에는 주무부장관은 필요한 한도 내에서 개인정보취급사업자에 대하여 개인정보의 취급에 관한 보고를 하게 하거나[108] 시정조치의 권고 또는 명령을 할 수 있는 것에 불과하다.[109]

2012년 EU Regulation	일본 개인정보보호법
제53조(권한) 1. 감독기관은 다음과 같은 권한을 갖는	제32조(보고의 징수) 주무장관은 이 절의 규정의 시행

106) 2012년 EU Regulation 제53조 참조.
107) 2012년 EU Regulation 제54조 참조.

108) 일본 개인정보보호법 제32조 참조.
109) 일본 개인정보보호법 제34조 참조.

다. (a) 개인정보 처리와 관련된 규정 위반에 대해 개인정보처리자나 수탁자에게 알리고, 해당되는 경우 정보주체의 보호 수준을 개선하기 위해 구체적인 방식으로 위반 사항을 시정하도록 개인정보처리자나 수탁자에게 요구한다. (b) 이 법안에 따라 제공된 권리를 행사하기 위한 정보주체의 요청에 따르도록 개인정보처리자나 수탁자에게 명령한다. (c) 개인정보처리자나 수탁자 그리고 해당되는 경우에는 대리인에게 의무 이행에 필요한 정보를 제공하도록 명령한다. (d) 제34조에서 언급한 사전 승인 및 사전 자문 규정의 준수를 보증한다. (e) 개인정보처리자나 수탁자에게 경고나 권고를 한다. (f) 이 법안을 위반하며 정보가 처리되는 경우 해당	에 필요한 한도 내에서 개인정보취급사업자에 대하여 개인정보의 취급에 관한 보고를 하게 할 수 있다.

되는 모든 정보의 수정, 삭제, 파괴를 명령하고, 정보가 공개되는 제3자에게 이러한 행동을 통지한다. (g) 처리에 대한 임시 또는 최종적인 금지를 결정한다. (h) 제3국의 수령인이나 국제기구로의 정보 이전을 보류한다. (i) 개인정보 보호와 관련된 의견을 제시한다. (j) 의회, 정부기관, 정치기구, 일반대중에게 개인정보 보호와 관련된 문제에 대해 알린다. 2. 각 감독기관은 개인정보처리자나 수탁자로부터 다음을 얻기 위한 조사권(investigative power)을 갖고 있다: (a) 의무 이행에 필요한 모든 개인정보와 모든 정보에 접근할 수 있는 권한; (b) 이 법안을 위반했다는 합리적인 근거가 있는 경우 개인정보처리자나 수탁자의 건물, 모든 정보처리	

장비 및 장치 등에 대한 접근 권한. (b)에서 언급한 권한은 유럽연합 및 회원국 법률에 따라 행사되어야 한다. 3. 제74조 (4)항 및 제75조 (2)항에 따라 각 감독기관은 이 법안의 위반 사항을 사법 당국에 이첩하여 사법 처리되도록 할 수 있는 권한을 갖고 있다. 4. 각 감독기관은 행정규정 위반 특히 제79조(4),(5),(6)에서 언급한 행정법규 위반에 대해 제재할 수 있는 권한을 갖고 있다.	
제79조(행정 제재) 1. 각 감독기관은 본 조(條)에 따라 행정제재(administrative sanction)를 부과할 수 있는 권한을 갖고 있다. 2. 각각의 경우에 대해 행정제재는 효과적이고 비례적이어야 하며, 추후 이 같은 위반을 억제할 수 있어야 한다. 과징금(administrative fine)의 액수는 위반의 성질, 위험, 기간, 침해가 고	제34조(권고 및 명령) ① 주무장관은 개인정보취급사업자가 제16조 내지 제18조, 제20조 내지 제27조 또는 제30조제2항의 규정에 위반한 경우 개인의 권리이익을 보호하기 위하여 필요하다고 인정되는 때에는 당해 개인정보취급사업자에 대하여 해당 위반행위의 중지 기타 위반을 시정

의적인지 또는 부주의에 따른 것인지에 대한 여부, 자연인 또는 법인의 책임 정도 및 이 사람이 이전에도 위반을 행했는지 여부와 그 책임 정도, 제23조에 따라 이행된 기술적 및 조직적 차원에서의 조치 및 절차, 위반을 시정하기 위한 감독기관과의 협력 정도 등에 따라 달리 결정된다. 3. 이 법안을 처음 또는 의도하지 않게 위반한 경우로써 다음의 경우에는 서면 경고가 주어지고 제재는 부과되지 않는다. (a) 자연인이 상업적 이익의 추구 없이 개인정보를 처리하는 경우; (b) 고용된 직원의 수가 250명 미만인 기업이나 단체가 주된 활동에 대한 부수적인 활동으로써 개인정보를 처리하는 경우. 4. 감독기관은 고의나 부주의로 다음을 행한 사람에게는 최고 250,000유로	하기 위해 필요한 조치를 취해야 한다는 취지를 권고할 수 있다. ② 주무장관은 전항의 규정에 의한 권고를 받은 개인정보취급사업자가 정당한 이유 없이 그 권고에 관계된 조치를 취하지 않는 경우 개인의 중대한 권리이익의 침해가 절박하다고 인정되는 때에는 당해 개인정보취급사업자에 대하여 그 권고에 관계되는 조치를 취하도록 명할 수 있다. ③주무장관은 전 2항의 규정에도 불구하고 개인정보취급사업자가 제16조, 제17조, 제20조 내지 제22조 또는 제23조제1항의 규정에 위반한 경우 개인의 중대한 권리이익을 해한 사실이 있어 긴급한 조치를 취할 필요가 있다고 인정되는 때에는 당해 개인정보

(EURO), 기업의 경우에는 연간 전 세계 매출의 0.5%까지 과징금을 부과한다. (a) 정보주체의 요청을 위한 장치를 제공하지 않거나, 제12조 (1)항 및 (2)항에 따라 정보주체의 요청에 신속하게 대응하지 않는 경우; (b) 제12조(4)항을 위반하며 정보에 대해 또는 정보주체의 요청에 대해 수수료를 부과하는 경우. 5. 감독기관은 고의나 부주의로 다음을 행한 사람에게는 최고 500,000유로(EURO), 기업의 경우에는 연간 전 세계 매출의 1%까지 과징금을 부과한다. (a) 제11조, 제12조 (3)항, 제14조에 따라 정보주체에게 정보를 제공하지 않거나, 불완전한 정보를 제공하거나, 투명하지 않은 방식으로 정보를 제공하는 경우; (b) 정보주체에게 접근을 허용하지 않거나, 제15조에	취급사업자에 대하여 당해 위반행위의 중지 기타 위반을 시정하기 위하여 필요한 조치를 취하도록 명할 수 있다.

따라 개인정보를 수정하지 않거나, 제13조에 따라 수령인에게 관련 정보를 전달하지 않는 경우; (c) 잊히거나 삭제되어야 하는 권리를 지키지 않거나, 시간제한이 준수된다는 것을 보증하는 장치를 실행하지 않거나, 제17조에 따라 개인정보의 모든 링크 삭제, 복사, 복제에 대한 정보주체의 요청을 제3자에게 알리기 위해 필요한 모든 조치를 취하지 않는 경우; (d) 전자 형식으로 개인정보의 복사본을 제공하지 않거나, 제18조를 위반하며 정보주체가 다른 곳으로 개인정보를 전송하는 것을 방해하는 경우; (e) 제24조에 따라 공동 관리자와 함께 부담하는 각각의 책임을 정하지 않는 경우; (f) 제28조, 제31조 (4)항 및 제44조 (3)항에 따라 문서로 적절하게 보관하지	

않는 경우; (g) 정보의 특정 범주가 관련되지 않는 경우로써, 제80조, 제82조, 제83조에 따라 표현의 자유와 관련된 규정이나 고용과 관련된 처리 규정, 역사, 통계, 과학 연구 목적을 위한 처리 조건 등에 관한 규정 등을 준수하지 않는 경우. 6. 감독기관은 고의나 부주의로 다음을 행한 사람에게는 최고 1,000,000유로(EURO), 기업의 경우에는 연간 전 세계 매출의 2%까지 과징금을 부과한다. (a) 처리에 대한 충분한 법률적 근거 없이 개인정보를 처리하거나, 제6조, 제7조, 제8조에 따른 동의 조건을 준수하지 않는 경우; (b) 제9조 및 제81조를 위반하여 특정한 범주의 정보를 처리하는 경우; (c) 제19조에 따른 반대(objection)나 요건을 준수하지 않는 경우; (d) 제20조에 따른 프로파	

일링(profiling)에 기초한 기준 관련 조건을 준수하지 않는 경우; (e) 제22조, 제23조, 제30조의 규정을 준수한다는 것을 보증하고 입증하기 위한 내부 정책을 채택하지 않거나 적절한 조치를 취하지 않는 경우; (f) 제25조에 따른 대리인을 지정하지 않는 경우 (g) 제26조 및 제27조에 따라 개인정보처리자를 대신한 처리와 관련된 의무 규정을 위반하며 개인정보를 처리하거나 처리하도록 지시하는 경우; (h) 제31조 및 제32조에 따라 개인정보 침해 사실을 적절히 또는 완전하게 감독기관이나 정보주체에게 경고 또는 통지를 하지 않는 경우; (i) 정보보호 영향평가를 실시하지 않거나, 제33조 및 제34조에 따른 감독기관의 사전 동의나 사전 자문 없이 개인정보를 처리	

하는 경우; (j) 정보보호 담당자를 지정하지 않거나, 제36조 및 제37조에 따른 업무를 이행하기 위한 조건을 보증하지 않는 경우; (k) 제39조에 따른 정보보호 인장(seal)이나 표시를 잘못 사용하는 경우; (l) 제40조 및 제44조에 따른 적절한 결정 또는 적절한 안전장치 또는 부분 수정에 의해 허용되지 않는 정보를 제3국이나 국제기관으로 이전하거나 이전을 지시하는 경우; (m) 처리에 대한 명령이나 임시 또는 확정적 금지를 준수하지 않거나, 제53조 (1)항에서 언급한 감독기관의 정보 이전 유보 조치에 따르지 않는 경우; (n) 제28조 (3)항, 제29조, 제34조 (6)항, 제53조 (2)항에 따라 감독기관을 지원하고, 감독기관에 대응하고, 감독기관에 관련 정보를 제공하고, 감독기관의	

건물에 대한 접근을 허용하는 의무 규정을 준수하지 않는 경우; (o) 제84조에 따른 업무 상 비밀 준수를 보증하는 규정을 준수하지 않는 경우. 7. 집행위원회는 제2항에서 언급한 기준을 고려하여 4항, 5항, 6항에서 언급한 과태료의 액수를 조정할 목적으로 제86조에 따라 위임된 법안을 채택할 수 있는 권한을 부여 받아야 한다.	

Ⅶ. 맺음말

앞에서 검토한 바와 같이 개인정보보호법은 법의 집행체계, 개인정보처리원칙, 당사자의 권리·의무 등 여러 면에서 외관상으로는 다른 나라 개인정보보호법과 유사해 보이지만 입법과정에서 다수이해당사자들과 일부 비전문가들의 의견이 반영되어 전체적으로 균형을 상실한 법이 되고 말았다. 클라우드 컴퓨팅 초래에 따른 네트워크 환경에서 정보주체의 권리를 좀 더 강하게 보호해야 할 부분에 대해서는 소홀히 하고, 글로벌 경제 환경에서 국제적 스탠더드를 존중해야 할 부분에 대해서는 지나칠 정도의 규제를 가하고 있다. 예산 절감 및 작은 정부라는 목표와는 달리 법집행주체를 다원화함으로써 고비용·비효율적인 집행체계를 탄생시키고 있다. 첫째, 개인정보보호법은 개인정보보호위원회라는 독립된 전문조직을 두면서도 개인정보보호와 관련한 권한과 역할을 보호위원회로 집중하지 않고 여러 부처·기관에 분산시킴으로써 행정력의 중복과 예산 낭비를 초래하고 있다. 또한 집행체계의 분산은 중복규제와 규제기준의 차이로 이어져 사업자와 소비자 등에게 혼란을 주고 있다. 둘째, 정보주체의 권리보호에 충실하지 못하다. 민감정보 및 고유식별정보 처리 제한에 대한 기준이 미흡하고 기본권 제한에 대한 법률유보원칙이 지켜지지 않고 있다. 또한 개인정보의 프로파일링화와 빅데이터화에 대한 대비도 미흡하다. 셋째, 제3자 제공 및 목적 외 이용에 대한 과도한 제한, 개

인정보처리의 사소한 변경에 따른 동의의무, 연구·개발 등 목적의 개인정보 처리제한 등에 대한 엄격한 법적용은 글로벌 경쟁력을 떨어뜨리고 있다. 이로 인해 법집행이 어려운 부분이 발생하고 있으며 국제적 스탠더드와 불일치하는 부분에 있어서는 국내기업에 대한 역차별 문제까지 우려되고 있다. 과잉규제는 불필요한 사회적 비용을 유발하며 과도한 컴플라이언스 비용을 발생시키므로 조속한 법 개정을 통해 합리적인 규제로 전환하여야 할 것이다.