情 報 保 護 學 會 誌
第22卷 第2號, 2012. 4

유럽의 개인정보보호 법 · 제도 동향

전 은 정*, 김 학 범**, 염 흥 열***

요 약

유럽연합(EU)이 출범하게 된 이후 OECD 가이드라인 및 유럽회의 조약에 맞춰 개인정보를 보호하는 국내법을 시행해 오던 유럽 각국이 입법수준이 다른 지역 내 시장에서 개인정보의 원활한 유통을 위해 EU차원에서의 지침을 1995년 10월 제정하였다. 이후에 유럽 각 국에서는 이 지침을 반영하여 자국 내에 개인정보보호 기구를 설치하여 운영하고 있으며 관련 법제도 등을 정비하는 등 개인정보보호에 많은 노력을 기울이고 있다. 본고에서는 영국, 프랑스, 독일, 네덜란드, 스웨덴 등의 유럽 국가에서의 개인정보보호 관련 기구와 법제도 추진 현황에 대해서 분석하였다.

Ⅰ. 서 론

1970년대부터 선진 각국에서는 컴퓨터와 정보통신기술의 발달로 인하여 발생하는 개인 프라이버시 영향에 주목하여, 이를 해소하기 위한 논의가 활발히 이루어졌다. 실제로 이러한 논의는 자국 내에서 행하여지는 개인정보의 자동처리를 규율함으로써 개인정보보호를 도모하기 위한 법제도를 확립하는 방향으로 진행되었다.

개별 국가 차원에서 논의되던 상황이 1980년대 들어 국제적 차원의 논의를 통하여 OECD는 1980년 프라이버시 보호와 개인정보의 국제적 유통에 관한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)을 제정하였다[1].

유럽연합(EU)도 1995년 10월 24일 개인정보의 보호 및 자유로운 이전에 관한 유럽의회와 이사회 지침을 마련한 데 이어, 1997년에는 통신부문의 개인정보처리 및 프라이버시 보호에 관한 유럽의회와 이사회 지침을 제정하였다. 이후 EU는 통신부문에 적용되는 97/66/EC 지침을 2002년 전자통신부문에서의 개인정보 처리 및 프라이버시 보호에 관한 유럽의회와 이사회 지침으로 대체하였다[2]. 유럽 각국은 EU 개인정보보호지침을 기반으로 각국에서 개인정보에 관련된 사항을 규정하고 있다.

본고에서는 유럽 각국에서 추진하고 있는 개인정보보호 관련 법제도 현황에 대해서 분석한다. 2장에서는 EU의 개인정보보호 지침 및 제도를 3장에서는 유럽 각국에서 추진하고 있는 주요 국가들의 개인정보보호 법제 동향에 대해서 살펴보고 4장에서 결론을 맺는다.

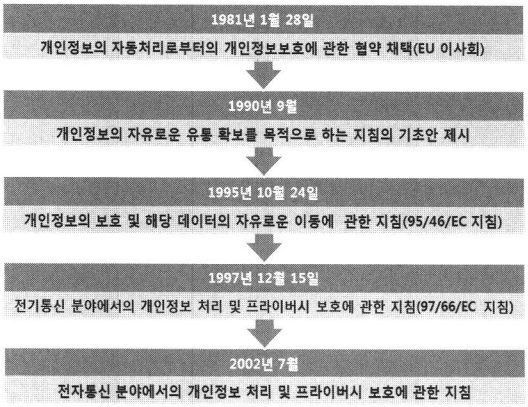
Ⅱ. EU 개인정보보호 지침 및 제도

2.1 EU 개인정보보호 지침

마스트리히트 조약이 1993년 1월 1일자로 발효됨으로써 유럽연합(EU)이 출범하게 된 이후 OECD 가이드라인 및 유럽회의 조약에 맞춰 개인정보를 보호하는 국내법을 시행해오던 유럽 각국이 입법수준이 다른 지역 내 시장에서 개인정보의 원활한 유통을 위해 1990년 9월에 EU차원에서의 국내법을 조정함으로써 개인정보의 자유로운 유통을 확보하는 것을 목적으로 하는 지침의 기초 안을 제의하였다. 이후 5년 후에 '개인정보 처리에 관한 개인의 보호 및 해당 데이터의 자유로운 이동에 관한 1995년 10월 24일의 유럽의회 및 이사회의 95/46/EC지침'(이하 'EU 지침'이라 함)이 채택되었다[1].

EU 지침은 자동처리 및 수동 처리된 '개인정보'의 처리에 적용된다. 여기에서 개인정보란 자연인을 직접 또는 간접적으로 식별 가능한 모든 개인정보를 말한다. 그러나 보도의 목적이나, 문학적 또는 예술적 표현의 목

* 순천향대학교 정보보호학과 (junej@sch.ac.kr)
** ㈜지엔에스인증원/동국대학교 국제정보대학원 (khb0305@gns-iso.co.kr)
*** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)



〔그림 1〕 EU 지침의 역사

적으로 행하여지는 음성 및 영상 정보의 처리(특히 시청각 분야)에 있어서는, 개인정보의 처리와 표현의 자유와 관련하여, 표현의 자유와 프라이버시권을 조화시킬 필요가 있는 경우에 한해 예외가 인정된다. 자동으로 처리되지 않고 수동으로 처리된 개인정보가 파일링시스템의 일부를 구성하는 경우에는 수동 처리된 개인정보에도 적용된다.

'파일링시스템'이란 일정한 기준에 따라 접속하는 것이 가능한 개인 정보의 집합을 구성하는 것이다. 그리고 '처리'란 수집, 기록, 축적, 번역, 검색, 참조, 이용, 배포, 삭제 또는 파기 등의 작업이 실행되는 것을 말한다. 그러나 공동체법의 적용범위 밖에서 개인정보가 처리되는 경우, 예컨대 공공의 안전, 방위, 국가안보, 형사법 분야에서의 국가 활동에 관하여 처리 작업이 이루어지는 경우, 또한 자연인에 의한 순수하게 개인적이거나 가정 내 활동 중에 처리되는 경우에는 개인정보보호지침이 적용되지 않는다. 자동 또는 수동 처리된 데이터는 어떤 조직과 단체가 보유해서 이용하는 것이지만, EU 지침의 적용대상이 되는 조직은 전자 또는 인쇄매체에서 개인정보를 보유하는 모든 조직 및 유럽연합과 유럽경제지역(EEA) 내의 모든 나라 사이에서 데이터의 이전을 행하는 기업이다.

EU 지침의 적용을 받는 지역은 유럽연합에 가맹하고 있는 15개국은 물론, 유럽경제지역에 대해서도 적용되는 한편, 비적용 범위는 중앙 및 동유럽 각국이다. 따라서 EU 지침의 적용을 받지 않는 나라는 유럽연합에 가맹하지 않는 한 본 지침이 말하는 제3국이 된다.

EU 지침의 특징은 공공부문과 민간부문의 구별을 하지 않고 있는 것이다. 또한 EU 지침은 EU 내부에서만

〔표 1〕 EU의 개인정보보호지침의 주요 내용[2]

구분	내용
적용범위	· 물적 범위 : 자동 처리되는 개인정보 및 구조화된 파일링시스템에 포함되는 개인정보 · 인적 범위 : 자연인의 개인정보
적용제외 영역	· 국가안보, 공공의 안전 및 방위를 위한 개인정보 처리 · 형사법 영역에서의 개인정보 처리 · 서신왕래와 같은 지극히 개인적이고 사적인 목적의 개인 정보 처리 · 언론보도, 문학, 예술적 표현을 위한 개인정보 처리
정보 처리자의 의무	· 공정하고 적법한 개인정보의 처리 · 정보처리 목적의 명시 · 정보처리 목적과의 적절성과 관련성, 비례성 유지 · 개인정보의 정확성과 최신성 확보 · 기술적, 조직적 보안조치 확보 · 감독기구에 정보처리에 대하여 고지
정보주체의 권리	· 정보처리의 전반적인 사항에 대하여 통지받을 권리 · 정보처리에 대하여 협의할 권리 · 자신의 개인정보에 대해 수정을 요구할 권리 · 특정 상황에서의 개인정보 처리에 대하여 반대할 권리
제3국으로의 정보이전 금지	· 적절한 보호수준을 갖추지 않은 제3국으로의 개인정보 이전 금지
독립기구의 설치	· 회원국 내 독립적인 개인정보보호기구의 설치

적용되는 성질을 가지고 있기 때문에 한국에 직접 영향은 없을 것이라고 이해하고, 유럽위원회가 교섭을 신청하였을 경우에 정부로서는 대응하는 것이 불가능하다는 우려가 있었다. 또한 EU 지침은 인터넷 기업의 동 지침의 위반에 대하여 어떤 경우에는 민사적 책임을 지울 뿐만 아니라 형사적 책임도 지우고 있으며 이사와 임원 등에 대해 별도의 책임을 묻기도 한다. 한편 EU 지침 제25조에서는 EU 회원국으로 하여금 EU 내의 개인정보의 보호뿐만이 아니고 적절한 보호수준을 제공하지 않는 비회원국으로의 정보의 이동을 금지하도록 하고 있다. 이에 따라 EU에서는 제3국이 업계의 자율규제(industry self-regulation) 또는 당사자 간의 계약(contract)에 의하여 개인정보보호가 적절하게 이루어지고 있다고 판단하는 경우에는 제3국으로의 정보이전을 허용하고 있다. 그 외에 EU에서는 특히 전기통신분야에 있어서 개인정보 보호를 위해서 '전기 통신 분야에 있어서의 개인 데이터 처리 및 프라이버시 보호에 관한 1997년 12월 15일의 유럽의회 및 이사회의 97/66/EC

지침'[3]이 제정되어 있으며 이 지침은 2002년 전자통신 부문에서의 개인정보 처리 및 프라이버시 보호에 관한 유럽의회와 이사회 지침[4]으로 대체되었다.

EU지침은 지역내에서 개인정보를 취급하는 경우에 항상 적용되는 것은 아니다. 동 지침에 의하면 개인정보의 처리를 전부 또는 일부 자동화 수단(automatic means)으로 하는 경우, 또는 개인정보를 자동화 수단 이외의 방법으로 처리하더라도 그것이 파일링시스템의 일부를 구성하거나 구성할 의도로 처리되는 경우에 적용된다. 즉 개인정보를 컴퓨터로 처리하거나 수작업(manual)으로 하더라도 개인에 관하여 일정 기준에 따라 구조화된 파일링시스템을 갖추게 되면 EU지침이 적용되는 것이다. 구체적으로 EU 회원국의 개인정보를 제3국에 이전하기 위해서는 동지침 제29조에 의하여 설치된 개인정보보호 작업반에서 설정한 일정한 기준을 따라야 한다. 왜냐하면 EU지침은 제25조 1항에서 제3국이 적절한 수준의 보호를 보장하는 경우에 한하여 정보의 이전을 허용할 수 있다고 규정하였기 때문이다. 다만, 다음과 같은 경우에는 적절한 수준의 정보보호가 이루어지지 않더라도 예외적으로 정보의 이전을 허용할 수 있다.

① 정보주체가 정보이전에 명백히 동의한 경우
② 정보주체와 관리자간에 체결된 계약의 이행에 필요한 정보이전 또는 정보 주체의 요청에 따른 계약 전 조치의 이행에 필요한 정보이전
③ 정보 관리자와 제3자간에 정보주체의 이익을 위한 계약의 체결 또는 그 이행을 위하여 필요한 정보이전
④ 중요한 공익상의 이유에 의한 또는 조세·사회보장 등 법적으로 의무화된 정보이전 또는 소송의 제기·수행·방어를 위하여 필요한 정보이전
⑤ 정보주체의 중대한 이익의 보호를 위하여 필요한 정보이전
⑥ 법령상으로 일반 공중이 열람할 수 있는 공부로부터 일정 요건을 갖춘 경우에 일어나는 정보이전. 이 경우 공부의 열람을 청구한 자가 제3국에 소재하는지, 열람행위가 정보이전에 해당하는지 여부는 문제되지 아니한다.

개인정보보호 작업반에서는 OECD 가이드라인을 반영하여 [표 2]와 같이 구체적인 개인정보보호의 원칙을 마련하였다.

〔표 2〕 개인정보보호 원칙

원칙	내용
목적 제한의 원칙	개인정보는 특정 목적을 위하여 처리되고 이용되며, 이전 목적에 반하지 않는 한 유통될 수 있다.
정보의 질, 비례의 원칙	정보는 정확하여야 하며 필요하면 갱신 되어야 한다. 정보는 이전·처리의 목적과 관련하여 적절하고 과도하지 않아야 한다.
투명성의 원칙	개인은 정보가 처리되는 목적과 제3국에서 당해 정보를 관리하는 주체, 기타 공정성을 확보할 수 있는 정보를 알 수 있어야 한다. 유일한 예외는 EU지침 제11조 2항과 제13조에 규정되어 있다.
안전성의 원칙	정보를 관리하는 자는 정보처리상의 위험에 비추어 적당한 기술적 및 관리적 보안 조치를 취하여야 한다. 그의 감독 하에 정보를 취급하는 자도 정보관리자의 지시를 따라야 한다.
열람·정정·거부의 권리	정보의 주체는 그에 관한 모든 정보를 열람할 수 있어야 하며, 부정확한 정보는 이를 정정하고, 일정한 경우에는 그에 관한 정보의 처리를 거절할 수 있어야 한다.
정보이전의 제한	개인정보를 수령한 자가 이를 다시 전송 하고자 할 때에는 제2의 정보수령자가 적절한 수준으로 이루어지는 개인정보 보호의 규정의 적용을 받고 있어야 한다.

EU는 위의 원칙에 추가하여 현실적으로 문제가 자주 일어나는 민감한 정보, 불특정 다수의 잠재고객에 대한 다이렉트 마케팅(DM), 그리고 컴퓨터에 의하여 자동적으로 정보이전이 정해지는 경우에 대비하여 다음과 같은 원칙을 보완하였다.

① 민감한 정보(sensitive data): 인종·정치적 신조·건강 등 민감한 정보에 대하여는 정보주체의 명시적인 동의(opt-in)를 요하여야 한다.
② 다이렉트 마케팅(DM): DM 목적으로 정보를 처리하는 경우에는 정보주체가 언제든지 자신의 정보를 제외(opt-out)시킬 수 있어야 한다.
③ 자동적인 결정: 정보이전의 목적이 자동적으로 결정되는 경우 이러한 결정 로직을 알고 정보주체의 이익을 보호하기 위한 조치를 취해야 한다.

이와 관련하여 정보주체의 권리행사 및 구제를 도울 수 있도록 다음과 같은 요건을 갖추어야 한다.

① 정보주체가 자신의 권리와 행사방법을 잘 알고, 정보처리자가 개인정보보호규정을 충분히 지킬 수 있어야 하며, 위반 시의 제재수단이 잘 갖추어져 있을 것
② 정보주체가 자신의 권리를 행사함에 있어 관련기

관·단체로부터 지원 및 조력을 받을 수 있을 것
③ 보호규정 위반 시에는 피해자에게 독립적인 분쟁 해결 또는 중재 시스템 등 적절한 구제수단이 제공될 것

EU 회원국을 비롯한 대다수의 선진국들은 높은 수준의 전자정부서비스를 제공하고 있으나, 전자정부서비스 제공을 목적으로 한 개인정보의 공유에 관하여 규정하고 있는 경우는 매우 드물다. 특히 EU의 경우에는 공공부문에서의 개인정보 공유나, 민간부문에서의 개인정보 공유나 서로 다를 게 없기 때문이다[5].

이상과 같은 EU의 개인정보보호 원칙은 미국과 차이가 있음에도 국제적인 기준으로 자리를 잡아가고 있다. 다시 말해서 유럽 모델이 상대적인 우위를 점하면서 비유럽 국가에까지 확산되고 있다. 이는 EU 회원국들이 개인정보보호가 미흡한 나라에 대해서는 정보의 유통을 금지하는 강경책에 기인하는 것이지만, 법률과 시장의 자율규제, 기술규약은 상호 유기적으로 영향을 미친다는 점에서 같은 방향으로의 조화로운 결합을 모색할 필요가 있는 것이다.

2.2 유럽의 개인정보보호기구[6]

유럽연합의 주요 국가들은 각 나라별로 EU 지침 준용과 각국에서 추진 중인 개인정보보호 규정 이행을 위하여 개인정보보호를 관장하는 기구들을 설립하여 운영하고 있다.

2.2.1 독일

독일의 연방 프라이버시 커미셔너(Bundesbeau-ftragter fur den Datenshutz)는 연방정보보호법('77) 및 전자통신법('96)에 근거하여 설립된 법정기구로 연방정부 및 공공기관, 연방정부 산하단체, 연방법원, 여러 주에 걸쳐 사업하는 우편이나 통신업자 등에 대해서만 관할한다.

2.2.2 오스트리아

오스트리아는 정보보호위원회와 정보보호자문위원회로 구분하여 운영하고 있다. 정보보호위원회(Data Protection Commission)는 공공분야의 개인정보침해 및 개인의 자기정보 접근요구에 대한 상담 및 신고를 접수받아 사실조사와 심리를 거쳐 결정하는 역할을 담당한다. 반면 정보보호자문위원회(Data Protection Council)는 정보보호 및 프라이버시와 관련된 중요한 정책문제 및 현안에 대하여 연방 및 주정부에게 자문을 행하는 역할을 담당한다.

2.2.3 그리스

그리스의 정보보호원(Hellenic Data Protection Authority)은 개인정보보호에 관한 법률에 따라 설립('97.11)되었다. 동 기구는 자국 내에서의 프라이버시 침해를 감시하기 위해 설립된 독립기구로서, 그리스의 개인정보보호법 및 모든 개인정보보호와 관련된 규칙의 이행여부를 감독하는 역할을 담당한다.

2.2.4 핀란드

핀란드의 정보보호옴브즈만(The Data Protection Ombudsman)은 개인정보보호법('99)에 근거하여 설립된 핀란드의 개인정보보호기구로 핀란드의 개인정보보호법을 집행하고 개인정보와 관련된 각종 불만 사항이나 신고를 접수받아 처리하는 역할을 한다. 또한 정보보호옴브즈만 외에도 정보처리 허가 등의 역할을 담당하는 정보보호위원회(The Data Protection Board)가 함께 운영되고 있다.

2.2.5 덴마크

덴마크의 정보보호원(Datatilsynet)은 정보위원회(Data Council)와 사무국으로 구성되어 있다. 정보보호원은 덴마크의 개인정보보호 기본법인 개인정보 처리에 관한 법률에 따라 민간부문과 공공부문의 모든 개인정보 관련문제를 다루고 있다.

2.2.6 영국

영국의 정보커미셔너(Information Commissioner)는 민간과 공공부문의 모든 개인정보처리를 감독하고 규제할 뿐 아니라, 정부 및 공공기관에 대한 정보공개가 원활히 이루어질 수 있도록 하는 업무를 하고 있다. 이 외

에도 의료정보, CCTV, 신용정보, 교육정보, 정보통신 분야, 근로자 정보, 다이렉트 마케팅 등 각 영역별 개인정보보호에 대해서도 각종 지침이나 규약의 제정을 통해 관할하고 있다.

2.2.7 네덜란드

네덜란드의 정보보호원(College bescherming persoonsgegevens)은 개인정보보호법에 따른 개인정보파일의 처리·운영을 감독하는 기구로 법 위반행위 또는 개인정보침해행위에 대하여 행정규제를 가하거나 벌금을 부과하는 등의 조치를 취하고 있다.

2.2.8 프랑스

프랑스의 국가정보처리자유위원회(Commission Nationale Informatique Libertes, CNIL)는 17명의 위원으로 구성된 합의제 독립행정기관으로 1978년 정보처리 축적 및 자유에 관한 법률을 기본으로 하여 기타 공공부문에서의 개인정보처리, 금융부문에서의 개인정보보호문제, 의료정보보호 등에 관하여 포괄적으로 관장하고 있다.

2.3 EU 개인정보보호 인증 서비스

2.3.1 TÜV라인란드 일본지사

TÜV라인란드일본(TÜV Rheinland Japan Ltd.)지사에서 'EU 개인정보 보호지침 인증 서비스'(EU Personal Data Protection Certification Service)를 첫 개시했다. 이 서비스는 EU 국가에서 EU 이외 지역의 제3국으로 개인정보를 전송, 처리할 때 적절한 기술·조직적 보호조치를 적용하고 있는지를 평가하는 것이다. 렉수스(Lexues Inc.)가 처음으로 해당 인증서를 받았다[7].

TÜV라인란드가 제공하는 'EU 개인정보보호 인증 서비스'는 EU 개인정보 처리에 관여하는 기관을 통해 귀사가 EU 지침과 EU 회원국 관련 법령에 명시된 요구조건을 충족했는지를 객관적, 효과적으로 확증한다. TÜV라인란드와 같은 제3자 인증기관으로부터 평가·인증을 받는 것은 시장에서 브랜드 이미지를 높이는 것은 물론, 경쟁력과 신뢰도를 높이는 효과도 있다.

2.3.2 BS 10012 인증

BS 10012 인증은 2009년 5월 31일 영국의 BSI가 발행한 BS 10012 "데이터보호-개인정보경영정보 시스템에 대한 표준(BS 10012 Data protection - Specification for a personal information management system)"[8]에 의해 2010년 1월부터 진행되고 있는 개인정보보호 관련 인증이다.

BS 10012는 개인정보의 효과적 관리를 위한 체계에 관한 표준으로써, 개인정보관리를 위한 기본체계 및 신뢰를 제공하고 컴플라이언스에 대한 평가를 위해 내부

〔표 3〕 BS 10012 규격의 구성

원칙	내용
범위	- 개인정보관리를 위한 기본체계 및 신뢰를 제공하고, 컴플라이언스에 대한 평가를 위해 내부 및 외부 평가가 효과적으로 이루어 질 수 있도록 함 - 조직 내 PIMS에 대한 수립, 책임, 구현 및 유지를 위함 - 공공 및 민간부문 등 조직 규모에 제한 없이 모든 조직에 적용 가능한 규격 - "Plan-Do-Check-Act"(PDCA) cycle을 적용 - DPA외 법규 참조
용어 및 정의	- Personal information management system - Personal Information (DPA 정의)
PIMS 수립	- PIMS의 Scope과 개인정보관리 목적 정의 - 개인정보관리 정책 수립 - 컴플라이언스 이행을 위한 책임과 역할 - 조직문화에 PIMS 적용
PIMS 구현	4.1 개인정보관리 담당자(책임자) 임명 4.2 개인정보 목록관리 4.3 교육과 인식 4.4 위험평가 4.5 PIMS 개선활동 4.6 Notification 4.7 공정하고 적법한 처리 절차 4.8 새로운 목적에 따른 개인정보 처리 4.9 목적에 부합하는 적절하고 관련된 정보처리 4.10 개인정보의 최신성과 정확성 유지 4.11 보유 및 파기 4.12 개인정보 소유자의 권리 4.13 기술적 보안통제 4.14 EEA(European Economic Area) 밖으로 전송되는 경우 보호(국외, 제3자 등) 4.15 제3자로의 공개 4.16 위탁시 계약 및 보안절차 4.17 유지관리 활동
PIMS 모니터링 및 검토	5.1 개인정보 처리에 대한 효과성 감사 수행 5.2 경영검토 수행
PIMS 개선	6.1 예방 및 시정조치활동 6.2 지속적인 개선활동

및 외부 평가가 효과적으로 이루어 질 수 있도록 하며, 조직 내 PIMS에 대한 수립, 책임, 구현 및 유지를 위함이다. 또한 공공 및 민간 부문 등 조직 규모에 제한 없이 모든 조직에 적용 가능한 국제규격이다.

활발하지는 않지만 인증이 진행 중이며, 국내 기업으로는 엔씨소프트가 전 세계 최초로 인증을 획득하였으며, 하나 SK카드, 윕스 등도 인증을 받았다.

BS 10012 규격의 구성은 [표 3]과 같다.

개인 정보의 효과적인 관리 조직에 도움을 주도록 설계 BSI의 데이터 보호 온라인이, 2009년 9월 16일에 발표되었다[9]. 또한 정보보호 및 IT 거버넌스 전문회사인 영국의 IT거버넌스社는 BS10012 표준을 이용하여 영국의 데이터 보호법 (DPA)를 준수할 수 있는 툴킷을 2010년 5월 출시하였다[10].

Ⅲ. 유럽 주요 국가들의 개인정보 법제 동향

유럽 주요 국가에서는 개인정보보호에 관한 법을 제정하여 시행 중에 있으며 각 나라별로 약간의 차이가 있다. 이 장에서는 스웨덴, 독일, 영국, 프랑스의 법제도 동향에 대해서 살펴본다.

3.1 스웨덴의 정보보호 법제

3.1.1 스웨덴 개인정보보호 법제의 발전

스웨덴의 1973년 Datalag(정보법 : The data Act, 1973: 289)은 개인정보에 관한 세계최초의 국내입법으로 알려져 있다. 그러나 개인정보에 대한 정확한 이해가 부족한 상태에서 입법이 이루어진 탓에 그 규제의 범위를 설정하는데 있어서 지나치게 포괄적인 규정을 둠으로써, 제정 당시부터 표현의 자유를 침해한다는 비판을 받아왔다. 실제로 1998년 10월에 새로운 법에 의하여 Datalag가 폐지되기 전까지 26차례나 개정되었으며, 그 중 개인정보보유자에 대한 허가규정인 제2조의 경우, 6차례의 개정이 있었고, 제 4조 역시 7차례나 개정되었다.

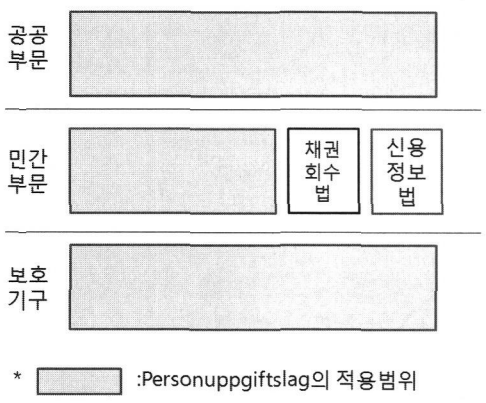
스웨덴의 Datalag에서는 개인정보를 개인과 관련된 정보라고 규정하여 개인과 관련된 일체의 정보는 이를 개인정보를 보고 있었다. 이러한 태도로 인하여 개인정보의 정의에 대하여 많은 비판이 있었다. 일반적으로는 특정 목적을 가지고 수집 축적되고, 개인에 대한 충분한 식별의 개연성을 가진 정보를 개인정보로 보아야 함에도 개인에 대한 아주 적은 개연성만을 가지고도 개인정보로서 규제할 수 있는 여지를 가지고 있었던 것이다. Datalag는 개인정보를 저장하고자 하는 경우에는 정보주체의 동의를 얻도록 하고 있었기 때문에, 이 E-mail에 언급된 제3자로부터도 동의를 얻어 이를 보관하여야 한다. 결국, 어떤 사람도 상대방을 비판하거나, 상대방 또는 제3자에 대한 부정적인 내용을 E-mail을 통해서는 전송할 수 없게 된다는 결론이 나오게 되는 것이다. 결국, 자동 처리되는 개인 정보에 대한 지나친 포괄규정은 언론의 자유는 물론 일반 국민의 표현의 자유까지 침해하게 되는 결과를 낳게 되었다.

인터넷상의 글들 중에서 대부분은 Datalag에 의하여 불법적인 것이지만 Datainspeltionen가 이를 직접 규제하거나 하는 경우는 거의 없었다. 다만 인터넷상에서 BBS를 운영하는 자가 이에 대한 허가를 신청하는 경우에만 이를 금지하도록 하는 방식을 취하였다. 결국 Datalag의 규정을 무시하고 BBS를 이용하는 경우에는 Datalag의 적용을 받지 않는 이상한 결과를 낳게 된 것이다. 결국, 언론 및 표현의 자유와 의 관계는 물론 법의 실효성에 대한 많은 의문이 제기 되었고 이러한 여파로 1998년 Datalag를 완전히 대체할 Personuppgiftslag가 제정되기에 이르렀다.

1998년 4월 제정된 Personuppgiftslag(개인정보법: Personal Data Act 1998:204)[11]는 기존의 Datalag를 전면 대체하는 새로운 법이다. 과거 Datalag의 규제에 의하여 언론의 자유 및 표현의 자유가 지나치게 제한된다는 것과 새로운 IT기술에 의한 개인정보의 침해에 대하여 충분한 보호와 이용의 규제를 할 수 없다는 반성에서 시작한 이 법의 제정은 1995년 EU Directive에 대한 검토로부터 시작되었다. 유럽 각국은 1995년 발표된 EU의 Directive에 의하여 개인정보의 보호에 관한 국내입법을 재정비하기 시작하였고, 이에 따라 스웨덴 역시 개인정보보호법제에 대항 전면적인 수정이 불가피하였던 것이다. 스웨덴은 EU의 Directive를 중심으로 타국의 입법례와 유사하게 Personuppgiftslag를 제정하였는데, 가장 눈에 띄는 변화는 개인정보와 관련된 여러 용어들에 대한 정의 규정이었다. 일반적으로는 사용되는 (개인정보의) 처리, 차단 , 개인정보 등 구법에서는 일반적인 용어로서 사용되는 어휘들에 대하여 정확한 정의규정을 두어 개인정보의 취급에 대한 포괄적 무분별

한 적용을 사전적으로 차단하도록 하였다. Personuppgiftslag의 구조를 보면 주로 개인정보가 어떻게 취급되어야 하는가에 대한 규정들로 이루어져 있는데, 과거의 Datalag가 개인정보의 취급에 있어서 Datainspeltionen의 허가와 규제 등, 감독기구의 역할에 관한 규정들이 대부분을 차지하던 것과는 매우 대조적으로 Personuppgiftslag는 개인정보의 적절한 이용과 보호에 중점을 두게 되었다. 또한 Datalag와는 순수한 개인 목적의 개인정보의 처리에 있어서는 동법의 적용을 배제하여 일반 국민의 자유와 권리를 침해하지 않도록 하였다.

스웨덴 개인정보보호법제는 크게 3개의 법률로 구성되어 있다. 먼저 기본법 내지 일반법으로서 앞서 설명한 Personuppgiftslag가 전 영역에서 이루어지는 개인정보에 관한 사항을 규제하고 개인정보보호기구인 Datainspeltionen의 업무에 대한 규정을 두고 있다. 공공부문에 대한 개인정보에 관해서는 이 Personuppgiftslag에 의하여 개인정보에 관한 사항이 적용되며, 민간영역에서는 채권회수법과 신용정보법이 개인의 신용과 관련된 개인정보에 관한 규제를 하고 있다.



〔그림 2〕 Personuppgiftslag의 적용범위

스웨덴 채권회수법(Inkassolag)은 채권회수업을 영위하는 자의 채무자에 대한 채권회수 업무에 대한 규제를 그 목적으로 한다. 이 법은 1974년 제정되었는데. 이 법과 관련된 사항의 감독기관은 Datainspeltionen이다. 동법에 의하면 채권회수업을 영위하는 자가 타인의 이익을 위하여 채권을 회수하거나 채권회수를 위하여 채권을 인수하는 때에는 Datainspeltionen에 의하여 허가를 받아야 한다. 이를 위하여 채권회수회사는 채권회수에 관한 자격이 있는 자를 고용하여야 하고, 이러한 조건의 준수여부에 대한 판단은 Datainspeltionen에서 이루어진다. 채권회수는 전문적 합법적인 절차에 따라 이루어져야 하며, Datainspeltionen은 이러한 규정의 준수여부에 대하여 감시 감독할 수 있다. 채권회수를 목적으로 수집된 개인정보는 당해 정보주체에 대한 객관적 사실 이외에는 가치판단이 개입되어서는 안 된다.

신용정보법(Kreditupplysningslag)은 신용등급기관에 의한 개인신용정보의 취급에 관한 규제를 목적으로 하는 법률로, 1973년 제정되었다. Personuppgiftslag에 의하여 규제되는 다른 분야들과는 달리, 신용정보 분야에 대해서 특별법이 존재하는 것은 스웨덴은 15세 이상의 모든 국민에 대한 신용정보가 신용등급회사에 의하여 수집 관리 되고 있기 때문이다. 이러한 이유로 스웨덴은 신용정보에 대해서만은 특별법을 제정하여 개인정보를 달리 규제하고 있다. 채권회수법과 마찬가지로 동법에 대한 관할관청은 Datainspeltionen이며 다음과 같은 사항을 규제한다. 신용등급기관은 법인의 재정적 상태 및 개인에 대한 재정적 인적환경에 대한 정보를 수집할 수 있다.

신용등급과 관련된 업무를 하고자 하는 자는 Datainspeltionen의 허가를 받아야 하며 신용등급 평가 행위는 적법한 절차에 의하여 이루어져야 하는데 Datainspeltionen은 이에 대한 감독권을 가진다. 개인과 관련된 특별한 사항은 신용가치에 대한 평가와 같이 법률적 사유가 존재하는 경우에만 제3자에게 제공될 수 있다. 이때에도 관련된 당사자는 제공된 정보의 사본을 열람할 권리가 있다. 신용평가기관의 과실은 당해 기관의 손해배상책임을 발생시키며 경우에 따라 벌금형 또는 징역형에 처해진다.

3.1.2 스웨덴 개인정보보호법의 주요 내용

다른 유럽 국가들과 마찬가지로 스웨덴 법률상에도 데이터 제공자의 동의가 있을 경우, 마케팅 목적을 위한 개인정보의 수집과 활용이 가능하다. 그러기 위해서는 광고자의 신원과 목적이 제공되어야 하며, 데이터 제공자들에게 개인정보의 사용을 명확히 해야 한다. 민감한 데이터는 종교나 인종, 정치, 성 관심도, 건강 그리고 Trade Union Member의 여부에 따라서 분류되는데, 중요한 공적 관심이 있을 경우, 정부는 민감한 정보 활용

의 금지 조약을 면제 시켜주기도 한다.

원칙적으로, 등록된 사람의 전송 동의나 아래의 사항에 의거한 전송 동기가 있지 않는 이상 가공된 개인 데이터의 제 3국가 (EU와 EEA이외의 국가)으로의 전송은 금지 되어있다. 하지만, 등록된 사람과 관리자와 의 특정한 계약이 있거나, 계약 이전에 등록된 사람의 평가가 있을 경우, 또는 등록된 사람이 관심을 갖고 있는 관리인과 제 3자의 계약 관계가 있을 경우에는 제 3국으로의 데이터 전송이 허가 된다. 개인 데이터 컴퓨터 프로세스에 관해서는, 만약 특정 국가에서 충분한 개인정보에 대한 보호가 이루어진다면, 정부는 개인 데이터의 전송에 대한 특정 규제를 발포 할 수도 있다. 관리자는 개인 데이터를 보호하기 위한 기술적, 운영적인 권리를 가지고 충분한 보안을 제공하는 측정치를 마련해야 한다. DIB(Data Inspection Board) 는 보안관련 전문, 보안에 관련 안내를 하고 보안 측정치를 결정하기도 한다.

관리자는 데이터 제공자의 요청에 의해, 개인 데이터 처리 과정에서 개인정보보호법(Personal Data Act) 또는

〔표 4〕 스웨덴 정보보호법의 주요 내용

원칙	내용
효력발생	1998. 10. 24. 발효
목적	개인정보처리로 인한 프라이버시 침해 방지(공공/민간)
경과 규정	과도기간을 두어 신법 발효 이전에 이루어진 행위에 대해서는 3년간(2001. 10. 24. 까지) 구법이 적용되도록 함
적용 범위	자동화된 개인정보 및 일부 수동처리된 개인정보파일의 처리(§ 5)
적용 배제	· 순수하게 사적으로 처리되는 개인정보(§ 6) · 공문서에 대한 공적 접근원칙, 언론의 자유, 표현의 자유에 해당하는 경우(§§ 7~8)
내용	· 개인정보처리에 관한 기본규정(§ 9) · 개인정보처리가 허용되는 경우의 규정(§ 10) · 민감한 개인정보에 대한 특별제한규정(§§ 13~19) · 개인정보의 정정, 처리과정상 보안에 관한 정보제공 규정(§§ 23~26) · 고지의무 : 개인정보를 처리하는 자는 DPB에 고지하여야 함(§ 36) · 고지의무의 면제 : 개인정보보호책임자가 임명되는 경우(§§ 37~38) - 개인정보보호책임자는 개인정보처리자의 정보처리 작용에 대하여 독립조사를 수행할 임무를 지님 · 강제적 고지사항 : 정보의 무결성과 관련하여 특히 민감한 특정 정보처리작용은 반드시 정보조사원에서 사전조사를 받기 위해 고지되어야 함(§ 41) · DPB의 권한 등에 관한 규정(§ 43)

규정을 어겼을 경우 데이터를 수정, 차단, 제한 또는 삭제를 실행할 의무가 있다. 만약 관리인과 등록된 사람간의 데이터의 수정 또는 아닌 것에 대한 논쟁 이 생일 경우 데이터 제공자는 이에 대해 DIB에게 보고 할 수 있다.

스웨덴의 개인정보보호법의 주요 내용은 [표 4]와 같다.

3.1.3 시사점

스웨덴의 개인정보법(Personuppgiftslag)은 현대 개인정보보호법제도의 발전에 있어서 다른 나라와는 다른 발전과정을 거쳐 왔다. 스웨덴은 세계 최고 수준의 행정국가로서 행정의 투명성을 정부운영의 최고의 가치로 삼고 있으며 이에 따라 국민의 행정기관에 대한 정보공개에 많은 노력을 기울이고 있다. 이에 따라 보호대상이 되는 개인정보와 공개의 대상이 되는 행정정보와의 관계를 해결하기 위한 노력의 결과로서 일찍부터 Datalag를 제정 시행하였다.

그러나 개인정보의 보호와 행정정보의 공개에 있어서의 철저한 규범 주의적 입장을 취하게 된 결과, 기타 분야에서의 정보보호와 정보의 자유로운 게시, 공개 등에 심각한 제한을 가져오게 되었고, 이에 따라 언론의 자유에 대한 심각한 침해로 인식되는 상황에 이르렀다.

스웨덴은 단일화된 성문헌법을 가지고 있지는 않지만, 4개의 법률에 헌법적 지위를 부여하고 있는데, 언론자유법과 표현의 자유에 관한 기본법을 헌법적 지위의 법률에 포함시켜 언론의 자유를 최대한 보장하고자 하는 스웨덴의 헌법정신이 Datalag에 의하여 훼손되었다는 평가를 받아오자, 이를 해결하기 위한 입법으로 Personuppgiftslag를 제정하게 된 것이다.

다른 나라가 개인정보의 이용 및 활용에 따른 privacy의 보호를 위하여 개인정보보호법제를 발전시켜 왔으나, 스웨덴은 이러한 개인정보보호를 위한 입법적 조치가 완료된 후에 언론의 자유, 표현의 자유와 관련한 상충관계를 해결하고자 하는 한층 더 보완된 개인정보보호법제를 가지게 된 것이다.

스웨덴의 법제도적 현황과 환경에 대해서는 아직 우리나라에 많이 소개되지는 못하고 있으나. 이러한 언론, 표현의 자유에 관한 시민의 권리와 프라이버시와 의 관계에 대한 스웨덴의 Personuppgiftslag의 제정 경과와 연구는 우리의 개인정보보호법제의 발전방향에서도 반드시 검토되어야 할 부분이라고 본다. 또한, 행정의 투명성에 따른 행정정보가 어느 정도까지 공개되어야 할

것이며, 이에 따른 개인정보의 보호문제에 대해서도 스웨덴의 경험은 우리의 개인 정보보호법제 발전에 큰 영향을 줄 수 있을 것이라고 본다.

3.2 독일의 개인정보보호 법제

3.2.1 연혁

1970년대 헤센주가 세계 최초로 개인정보보호법을 입법화한데 이어 1977년 연방정보보호법이 제정되었다. 이어서 연방정보보호법을 기초로 각 주의 개인정보보호법이 제정되었고, 연방 및 각 주에 개인정보보호관이 투입되고 이를 감독하기 위한 개인정보보호기구가 설립되었다.

그 후 이법은 연방헌법재판소의 인구조사판결, 정보통신기술의 발달, 적용과정에 나타나는 문제점 등으로 개정필요성이 강하게 제기되었고 이에 따라 연방정보보호법은 1990년 개정되었다. 이후 1995년 제정된 EU의 개인정보지침을 반영하기 위한 제3차 연방데이터보호법 개정작업이 착수되었다. 원래 지침에서는 1998년까지 기한이 주어졌으나, 독일은 2001년이 되어서야 개정작업이 마무리되었다. 그 이유는 EU의 개인정보보호지침의 반영이라는 1단계 목표뿐만 아니라 연방정보보호법의 현대화라는 2단계 목표를 갖고 있었기 때문이다.

이후 2010년 4월 1일에 발효된 개정법은 신용정보기관에 대한 정보의 전달 및 자동화된 개별결정(Automatisierte Einzelentscheidung)에 대한 내용을 포함하고 있으며[12], 개인채무와 관련하여 신용평가기관에 제공할 수 있는 개인정보의 종류를 명확히 하였다[13].

2011년 5월 23일 연방정부는 「근로자의 개인정보보호에 관한 법률안」을 하원에 제출하였으며, 이는 연방정보보호법 제3조 제11항 상에 규정된 근로자(Beschäftigte) 보호를 위한 실체적인 규정을 제정하기 위한 것이다[14].

〔표 5〕 독일의 개인정보보호관련 법제 연혁

연도 및 내용	주요특징
Hessen 주법 제정(1970)	세계 최초의 입법화
연방정보보호법 (BDSG) 제정(1977)	연방 차원의 개인정보보호에 관한 기본법
연방정보보호법 개정(1990)	BGB1.I 1990 S.2954
연방정보보호법 개정(2002)	EU 지침 반영
연방정보보호법 개정(2006)	- BGB1.I 2006 S.1970 - 개인인정보보호기관의 명칭 변경
연방정보보호법 개정(2010.4)	- 자동화된 개별 결정의 내용 포함 - 개인채무와 관련하여 신용평가기관에 제공할 수 있는 개인정보의 종류 명시
근로자의 개인정보보호에 관한 법률안 제출(2011.5.)	근로자 보호를 위한 실체적인 규정을 제정하기 위함

3.2.2 독일 개인정보보호법의 주요 내용

독일의 연방정보보호법은 제2장에서 '정보주체의 권리'라는 제목 하에 정보주체의 접근권(제19조·제34조), 통지받을 권리(제19a조), 정정·삭제·차단 요구권(제20조·제35조), 이의제기를 할 권리(제20조제5항)에 대하여 규정하고 있다. 특히, 제6조에서 정보주체의 이러한 권리는 계약 등 다른 법률행위에 의해 배제되거나 제한될 수 없는 불가침의 권리임을 명백히 밝히고 있다는 점에 그 특색이 있다.

정보주체는 개인정보의 처리에 있어서 권리침해가 있다고 믿는 경우에는 정보보호관찰관에게 이의신청을 할 수 있다(제21조). 일반적인 손해배상 책임에 관하여 규정하고 있는 제7조와는 달리 제8조는 공공부문에서의 정보처리로 인한 손해배상 책임에 관하여 규정하고 있는바, 공공부문이 개인정보를 위법 또는 부당하게 수집·가공 또는 이용한 경우에는 무과실책임을 부담하게 되며, 정보주체는 이 경우 중대한 인격권 침해가 있는 때에는 위자료의 배상을 청구할 수 있도록 하고 있다.

한편, 동법은 개인정보처리자가 준수하여야 할 의무사항에 대하여 규정하고 있는바, 개인정보처리자는 우선 제4d조제1항에 따라 연방정보보호청에 개인정보 처리행위와 관련된 소정의 사항을 고지하고 등록할 의무를 부담한다. 즉, 소관 감독기구의 사적 책임자, 연방정부의 공적 책임자, 우편 및 통신회사는 자동화된 개인정보 처리절차를 실행하기 전에 반드시 연방정보보호청에 소정의 사항을 신고하여 등록하여야 한다. 이는 정보처리를 위해 내부의 개인정보관리책임자를 임명하여야 하기 때문에, 상당수의 정보처리자가 이러한 등록의무에서 면제된다고 볼 수 있다. 다만, 정보처리자가 영리의 목적으로 정보를 전송하기 위해 또는 익명화된 정보를 전송하기 위해 개인정보를 저장하고 있는 경우에는 등록의무의 면제사유에 해당되지 않게 된다(제4d조제4항).

그러나 이러한 등록의무는 해당 개인정보처리자가

내부적으로 개인정보관리책임자를 임명하였을 경우에는 면제된다(제4d조제2항).

동법 제4f조에 따르면, 자동화된 개인정보파일을 처리하는 모든 공공·민간기관 또는 비자동화된 정보파일을 처리하는 곳이라도 최소 20명 이상의 인원이 고용된 단체에서는 개인정보처리를 위해 내부의 개인정보관리책임자를 임명하여야 하기 때문에, 상당수의 정보처리자가 이러한 등록의무에서 면제된다고 볼 수 있다. 다만, 정보처리자가 영리의 목적으로 정보를 전송하기 위해 또는 익명화된 정보를 전송하기 위해 개인정보를 저장하고 있는 경우에는 등록의무의 면제사유에 해당되지 않게 된다(제4d조제4항)[15].

3.2.3 특징 및 시사점

독일 연방데이터보호법은 개인의 정보에 관하여 공적 사적 영역을 구분하지 않고 동일한 법체계에서 보호하고 있다. 그리고 연방데이터보호법과 각 주의 개인정보보호법은 개인정보보호에 관한 특별법에 대하여 보충적으로 적용되는 일반법의 성격을 가지고 있다. 주요한 특별법으로는 통신법과 통신서비스개인정보보호법을 둘 수 있다. 통신법의 적용범위는 통신수단을 이용하여 정보를 전송 및 수령하는 모든 기술적인 절차를 포함하며 기본권으로 보장하고 있는 통신비밀의 보호를 구체화하고 있다. 또한 통신서비스개인정보보호법은 정보통신서비스를 이용하는 경우에 개인정보보호에 관한 규정들을 담고 있다. 이러한 정보통신서비스에는 텔레뱅킹, 전자우편 등의 개인통신들이 포함된다.

개정된 독일의 정보보호법은 몇 가지 특징을 지니고 있다.

첫째, 법 적용의 범위가 크게 확대되었다는 점이다. 다시 말해서 개인관련정보는 정보의 조사로부터 처리(저장, 변경, 전달, 삭제, 이용)을 거쳐 익명화 할 때까지 보호되고, 정보의 조사와 이용이 포함됨으로써 정보처리 이외의 모든 개인관련정보의 사용이 정보이용을 뜻하게 되었다. 그리고 개정된 법에서는 공공기관이 보유하고 있는 정보와 자료 가운데 자동화된 정보처리뿐만 아니라 서류들도 그 적용 범위에 포함시키고 있다.

둘째, 정보자기결정권을 보호하기 위하여 개인관련정보를 처리하고 이용할 때 목적구속원칙이 엄격하게 규정되었다는 사실이다. 과제수행을 위하여 필요하고 처리목적을 위하여 행해지고 조사되는 경우에만 개인관련정보의 저장, 변경, 이용이 허용되고 수신인은 전달받은 목적만을 위해서 그 정보를 처리하거나 이용하여야 할 것을 명시하고 있다.

셋째, 개인정보관련자의 권리가 여러 측면에서 향상되었다. 자기에 관한 정보처리와 저장 기관을 통한 이용에 관하여 알 수 있기 위하여 관련개인에게 인정되는 설명권은 개인정보를 보호하기 위해서는 매우 중요한 통제권이다.

넷째 컴퓨터 연결을 통한 직접 호출절차는 정보가 교환되는 관련자의 이익이 고려되고 해당기관의 과제측면에서 필요한 경우에만 허용되도록 함으로써 자동화된 호출절차로부터 개인정보를 보호하는 규정이 도입되었다. 따라서 정보전달의 원인, 목적, 정보수신인, 종류 등이 문서로 확인되도록 하였다.

3.3 프랑스의 개인정보보호 법제

3.3.1 연혁 및 현황

프랑스에서의 법 및 제도 현황에 관한 내용은 'Legal Fact Pack 2006'에 1974년 사파리(SAFARI) 법안에 대한 여론의 반발로 인해 공공부문과 민간부문에서 이루어지는 정보처리 기술 발달에 대비해서 개인의 사생활과 자유보호를 위해 방안을 강구하기 위하여 법무부 내에 위원회를 설치하였다. 위원회에서는 개인정보보호 기본법 제정 및 동법의 적용을 감독하는 임무를 맡는 독립적인 기구의 설치를 주장하는 보고서를 발표한 바 있다[16].

1978년 1월 6일 Loi relative à L'Informatique, aux fichiers et aux libertés 라고 불리는 The Data Protection Act No. 78-17 이 프랑스의 정보처리 축적 및 자유에 관한 법률의 제정으로 이어지게 되었다. 동법은 프랑스에서 이루어지는 모든 정보처리에 관한 사항을 규율하는 포괄적이고도 가장 기본적인 원칙을 확립함과 아울러, 의료정보를 비롯한 다양한 영역의 개인정보를 보호하기 위한 세부시행규정을 포함하고 있는데, 이를 살펴보면 [표 6]과 같다.

개인정보법(정보처리축적 및 자유에 관한 법률)을 토대로 하여 그 이후 개인정보보호를 위한 국제규범들이 공공부문과 민간부문을 구분하지 않고 모두 그 보호대

〔표 6〕 정보처리축적 및 자유에 관한 법률 및 하위규정[5]

구분	법규
기본규정	정보처리축적 및 자유에 관한 법률(Loi n° 78-17 du 6 janvier 1978, Loi relative àl'informatique, aux fichiers et aux libertés)
형사제재에 관한 규정	동법제41조~제44조
	형법제226-16조~제24조(Code Pénal Article 226-16 á24)
	시행령 81-1142 (Décret 81-1142 du 23 décembre 1981)
세부적용에 관한규정	법적용에 관한 시행령(Décret 78-774 du 17 juillet 1978)
	국가안보를 위한 개인정보처리에 관한 시행령 (Décret 79-1160 du 28 décembre 1979)
	접근권 행사시 부과금에 관한 시행령 (Décret 82-525 du 16 juin 1982)
	의료정보에 관한 시행령(Décret 95-682)
	개인건강정보의 처리에 관한 시행령 (Décret 99-919 du 27 octobre 1999)
	부과금 계산에 관한 시행규칙 (Arrêté du 23 septembre 1980)
	공공부문에서의 법적용에 관한 행정 통첩 (Circulaire du 23 mars 1993)

상으로 규정하는 등 최근 이 법률은 1995년 10월 24일 유럽인 법령 95/46/EC 의 효력을 부여하는 법안을 통해 프랑스 법으로 제정되었고, 위의 법안은 J.O No 182에 나와 있듯이 2004년 8월 7일 발표에 이르기까지 6차례의 변화를 겪게 되었다[16].

3.3.2 정보주체의 권리 및 의무

동법에 따르면, 정보주체는 수집 이전 또는 이후의 정보처리에 대하여 반대할 권리(제26조), 자신에 관한 정보수집에 대하여 고지 받을 권리(제27조), 자신에 관한 정보를 보유하고 있는지 여부를 정보처리자에게 물어보고 접근할 수 있는 권리(제34조 및 제35조), 정보처리자에 대하여 자신에 관한 정보의 정정·추가·명확화·갱신 혹은 말소를 청구하고, 해당 정보의 수정·삭제에 대하여 통지를 받을 권리(제36조 및 제37조) 등을 행사할 수 있다[1].

만약 정보처리자가 이러한 의무를 위반한 경우에는 벌금 또는 징역형에 처해진다. 특히 프랑스형법(Code Pénal) 제226-18조는 사기·신의 성실위반 기타 불법적인 방법으로 개인정보를 수집·처리하거나, 정보주체의 명시적인 반대의사에도 불구하고 정보를 수집·처리하는 자는 최고 5년의 징역 또는 300,000 유로의 벌금에 처해진다고 규정하고 있어, 정보주체의 반대할 권리를 실질적으로 보장하고 있다.

2011년 7월에는 「개인정보 보호법안(Proposition de loi relative à la protection l'identité)」이 프랑스 하원에 제출되어 검토 중이다. 이에 대한 주요 내용은 다음과 같다[17].

① 기존 신분증에 포함되어 있는 성명·성별·생년월일·출생지·주소지·신장·눈동자 색깔·디지털 지문·사진 등의 정보를 전자 보안 시스템으로 보호

② 이용자는 정보통신망에서 신분조회 및 전자서명 시 이용·전송될 자신의 개인정보를 선택

③ 이용자가 개인정보 이용에 동의하지 않았다는 이유로 전자정부 서비스 이용에 있어 제한을 받아서는 안 된다는 규정

④ 전자 신분증 관리를 위하여 통합 데이터베이스를 사용할 것을 규정

3.4 영국의 개인정보보호 법제

3.4.1 영국의 데이터보호법의 제정 연혁

영국에서는 1984년 정보보호법(The Data Protection Act 1984)을 제정함으로써 개인정보보호를 위한 발판을 마련하였다고 볼 수 있다. 그러나 동법은 개인정보보호를 위한 일반원칙을 모두 아우르고 있다기보다는 개인정보를 처리하는 공공기관이나 사업자 등을 등록하여 정보처리자 등록부를 유지·관리하는 것에 더 큰 초점이 맞추어져 있었다[1].

그러던 중 1995년 EU의 개인정보보호지침이 제정되면서, 영국도 동 지침의 내용에 맞추어 국내법을 전면 수정할 필요가 생겼던바, 이러한 배경 하에서 제정된 법률이 바로 1998년 정보보호법(The Data Protection Act 1998)이다.

1984년 법의 특징은 데이터주체의 권리로서 접근권을 인정하지만 그 적용범위를 자동처리데이터에 한정하고 있으며 데이터주체의 액세스가 작용되지 않은 영역도 규정하고 있었던 것이다. 따라서 그 후 개인의 접근권을 요구하는 운동이 일어났으며 이것의 성과로 자기정보에 대한 접근권을 인정하는 세 가지의 제정법이 성립되었다. 1987년 개인기록접근법 1998년 의료보고접근법 1990 보건기록접근법 등이 그것이다. 이들 법에서

〔표 7〕 영국의 개인정보보호관련 법제 현황[5]

분야	관련 법
개인정보	· 1998년 정보보호법(The Data Protection Act 1998)
정보공개	· 2000년 정보공개법(The Freedom of Information Act 2000)
전자통신 분야의 정보보호	· 1999년 전자통신규칙(정보보호 및 프라이버시)(The Telecommunications (Data Protection and Privacy) Regulations 1999 (1999/2093) · 2000년 조사권에 관한 법률규칙(The Regulations of Investigatory Powers Act 2000)(RIPA 2000) · 2000년 전자통신규칙(합법적인 사업관행)(통신차단) (The Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 (2000/2699))
신용정보	· 1974년 소비자신용법(The Consumer Credit Act 1974)
형사기록	· 1997 경찰법(The Police Act 1997)
의료정보	· 1988년 의료기록 접근에 관한 법률(The Access to Medical Reports Act 1988) · 1990년 건강기록 접근에 관한 법률(The Access to Health Records Act 1990)

는 컴퓨터에 의해 처리되는 정보는 물론 마이크로필름, 정보카드, 정보인덱스 등 수기 처리 정보도 포함하게 되었다. 1984년 데이터보호법과 1987년 개인기록접근법은 1998년 데이터보호법이 제정됨으로써 통합되었다.

EU지침의 제정에 따라 EU가맹국들은 이에 관한 국내법의 정비를 단행하였는데, 이탈리아에서 1996년 12월 31일 개인데이터의 처리에 관한 개인 및 다른 주체의 보호에 관한 법률이 제정된 것을 비롯하여 2001년 5월 독일의 연방데이터보호법이 성립하기까지 프랑스

〔표 8〕 영국의 개인 데이터에 대한 접근을 보장하는 법

제목	주요 내용
개인기록 접근법 (1987년)	· 지방자치단체 개발공사 스코틀랜드 특별주택협회가 보유하고 있는 주택임대차에 관한 개인정보 및 사회사업당국이 보유하고 있는 개인정보에 대한 개인의 접근을 인정 · 이는 개인데이터의 오남용으로부터 데이터주체를 보호하기 위한 제도임.
의료보고 접근법 (1988년)	· 고용 또는 보험계약의 경우에 의사로부터 교부된 환자의 의료기록에 대한 환자 자신의 접근권을 인정함
보건기록 접근법 (1990년)	· 환자의 권리의 하나로서 주장되어 온 의료 보에 대한 일반적 접근권을 인정한 법률 · 개별입법에 의해 특정분야에서의 자기정보에 대한 접근을 인정하는 것으로, 사적 의료 공적 의료를 묻지 아니하고 또 의사뿐만 아니라 기타 보건전문가가 보유하는 환자의 의료정보에 대한 접근을 인정함

를 제외한 거의 모든 EU 가맹국에서 이 지침에 따라 개인정보 전반은 대상으로 한 보호법제가 정비되었다. 1995년 10월 24일 제정된 EU지침은 EU가맹국으로 하여금 3년의 전환기간을 주어 EU지침에 따른 개인정보보호법을 정비하도록 하였으며, 이에 이 전환기간을 지킨 나라는 이탈리아, 그리스 및 영국, 스웨덴, 포르투갈 등이었는데 EU를 견인하는 양축을 이루는 나라 중 하나인 독일은 2001년 5월 신법이 성립되었으며, 프랑스는 2003년 4월 당시에는 전화의무를 지키지 않고 있었다.

이와 같이 영국은 EU를 이끌어 가는 영국, 독일, 프랑스의 3국 중 유일하게 전환기내에 국내법을 제정한 나라이며, 또 영국의 데이터보호법은 EU의 지침의 거의 모든 요구사항을 수용하고 있는 것이 특색이다. 1998년 법 개정에서 가장 흥미로운 점은 등록제에서 신고제로 바뀌었다는 점이다. 개인데이터의 자동처리를 등록하는 제도는 당시 파탄지경에 있어 완전히 폐기할 예정이었으나, EU지침에 따라 신고제를 채용하지 않을 수 없었던 것이다.

3.4.2 정보보호법의 적용범위 및 정보보호의 원칙

2000년 3월 1일부터 시행된 정보보호법은 영국의 개인정보보호에 관한 기본법으로서의 역할을 하고 있다.

개인정보보호의 기본원칙을 비롯하여 정보주체의 권리와 정보처리자의 의무, 개인정보보호기구의 설립 및 운영, 정보법원(Information Tribunal)의 설치, 개인정보의 국외이전 등에 관한 사항을 포괄적으로 규정하고 있다. 또한 적용범위에 있어서도 공공과 민간의 구분이 없다. 특히, 동법은 주로 전자적인 형태로 처리되는 개인정보를 규율할 목적으로 제정된 것이나, 그 후 적용범위가 더욱 확대되어 특정의 구조화된 수기 파일링시스템(manual filing systems)은 물론, 의료기록이나 교육기록에 대해서는 순수하게 수기로 처리되는 개인정보까지도 동법의 규율을 받는 것으로 하고 있다. 한편, 동법은 생존하고 있는 개인에 관한 정보를 보호대상으로 함을 명시적으로 밝히고 있다. 따라서 법인의 정보나 사자(死者)의 정보는 동법의 보호대상에서 제외된다.

동법의 가장 큰 특징은 개인정보의 수집 · 처리 등을 규율하기 위한 정보보호 8원칙을 세부적으로 규정하고 있다는 점이다. 이 원칙은 기본적으로 OECD의 프라이버시 8원칙과 유사하나, EU의 개인정보보호지침의 내용을 반영하여 개인정보 의 국외이전 제한의 원칙을 규

〔표 9〕 영국의 정보보호 8원칙[5]

원칙	주요 내용
제1원칙	공정하고 합법적인 개인정보 처리 및 민감한 정보의 특별처리
제2원칙	제한된 목적 내에서의 개인정보 처리
제3원칙	목적과의 적절한 관련성을 가진 개인정보의 처리 및 과도한 개인정보 수집·처리 금지
제4원칙	개인정보의 정확성 확보 및 필요한 경우 최신성 확보
제5원칙	수집목적 달성을 위한 필요한도 내에서의 보유
제6원칙	정보주체의 권리를 존중하는 방법을 통한 개인정보 처리
제7원칙	적절한 기술적·관리적 조치를 통한 권한 없는 접근·수정·손실 등으로부터 개인정보보호
제8원칙	적절한 개인정보보호수준을 갖춘 국가 이외의 곳으로 개인정보 이전금지

정하고 있으며, 민감한 개인정보에 대하여는 특별한 처리를 하도록 하고 있다는 점도 그 특징으로 들 수 있다.

3.4.3 주요내용 및 동향

동법은 정보주체가 개인정보자기결정권과 관련하여 어떠한 권리를 향유하는지를 구체적으로 밝히고 있다. 동법에서 보장하고 있는 정보주체의 권리를 살펴보면 다음과 같다[18].

① 자신의 정보에 접근할 권리
② 부정확한 개인정보를 정정·삭제할 권리
③ 자신에 관한 정보가 처리되고 있는 목적·방법·내용 등에 대하여 고지 받을 권리 및 이를 통해 자신과 관련된 정보의 처리에 대하여 반대할 권리와 같은 일반적인 정보주체의 권리
④ 다이렉트 마케팅의 목적으로 자신의 정보를 이용하는 것을 배제할 권리
⑤ 개인정보 침해로 인해 입은 피해에 대하여 보상을 받을 권리
⑥ 자신에 관하여 전적으로 자동화된 방법에 의한 의사결정이 이루어지는 것에 반대할 권리
⑦ 개인정보 침해행위가 있다고 판단될 경우 이의제기를 할 권리
⑧ 개인정보 처리의 법규위반 여부 심사를 청구할 권리 등이다.

2008년 6월 발표된 'Data Handling Review'에서는 개인의 정보보호를 포함한 정보 보안에 대한 인식의 변화를 강조하고 있다. 변화는 다음과 같은 네 가지로 정리할 수 있다. 첫째 모든 공공영역에 정보보호와 관련하여 의무적 감사를 실시하고, 둘째 개인정보를 취급하는 30만 명 이상의 공무원들이 의무적으로 관련교육을 받고, 'Cabinet Office'는 개인프라이버시 영향 평가를 실시한다. 셋째 각 부처별로 정보 보안에 대한 기준 강화 및 책임소재를 분명히 하고, 넷째 각 부처별로 해마다 정보위험을 어떻게 관리했는지 보고하여야 한다. 중앙정부 차원에서의 이러한 정보보호의 중요성에 대한 인식은 고위 공무원들에게도 널리 확산되어 가고 있다[19].

Ⅳ. 결 론

유럽의 EU지침 발효 이후에 유럽 각국에서는 이전에

〔표 10〕 유럽 국가의 개인정보보호 법제 비교

국가	대상정보	정보처리의 원칙	정보주체의 권리
스웨덴	전과정 또는 부분적인 과정이 자동화된 개인정보의 처리	· 언론의 자유, 표현의 자유와 관련한 상충관계를 해결하고자 하는 한층 보완된 원칙	· 동의철회권 · 주기적통보권 · 자동화된 결정권 · 정정요청권 · 삭제권 · 손해배상 청구권
독일	개인데이터와 관련하여 인격의 침해로부터 개인보호를 목적으로 하는 수작업 정보포함 공공부문의 데이터 파일형식 및 서류형식 민간부문의 데이터파일 형식에 적용	· 소관사무의 수행에 필요한 경우 법률 또는 동의에 의해 데이터 수집, 처리 및 이용 허용 직접성의 원칙 · 필요성의 원칙 · 정확성의 원칙 · 소거의 원칙 · 저널리즘 목적인 경우는 제외	· 데이터주체에 대한 통지 열람권 · 민간부문에 대한 데이터 통제권 · 이의신청권 · 입증책임의 전환
영국	공공 및 민간 부문의 기본법 자동 처리된 정보 및 관련 파일링 시스템의 일부로서 처리된 수작업처리 데이터 포함	· 동의의 원칙 · 목적제한의 원칙 · 상응성의 원칙 · 정확성의 원칙 · 보존필요성의 원칙 · 데이터 주체의 권리의 원칙 · 안전보장 조치의 원칙	· 액세스권 · 손해배상 청구권 · 금지청구권 · 자동화된 결정에 참가할 권리 · 정정권 · 봉쇄권 · 말소권 · 파기요구권
프랑스	수작업정보포함 공공, 민간부문 포함하여 자동처리된 정보에 중점 정보처리 시스템의 설치에 대한 규제	· 위법수집금지의 원칙 · 데이터처리거절권의 원칙, 사전통지의 원칙 · 보존필요성의 원칙 · 안전보호조치의 원칙 · 동의적 정보수집 제한의 원칙	· 광범위한 액세스권 · 정정, 추가 명확화, 갱신 · 말소청구권

추진하였던 다양한 관련법들을 EU지침을 반영하여 개정하였고 각국에 특성에 맞추어 개인정보보호 법제도를 운영하고 있다. 본고에서는 EU지침에 대한 소개와 함께 유럽 각국 특히 스웨덴, 독일, 프랑스, 영국을 중심으로 개인정보보호 관련 법제도 현황을 분석하였으며 주요 특징을 정리하면 [표 10]과 같다.

향후 국내에서도 현재 발효 중인 개인정보보호법의 시행 과정에서 생길 수 있는 문제들을 이미 제도를 시행중인 유럽 각국의 제도를 모니터링 함으로써 보완하여 좀더 실효성 있는 제도 운영이 될 것으로 사료된다.

참고문헌

[1] 김기열, "공공부문에 관한 외국의 개인정보보호 법제와 국내 입법의 검토 방향", 월간 법제, 2010. 9.

[2] 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.

[3] DIRECTIVE 97/66/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

[4] DIRECTIVE 02/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[5] 이창범, 윤주연, *각국의 개인정보피해구제제도 비교연구*, 개인정보분쟁조정위원회, 2003. 12.

[6] http://privacy.kisa.or.kr/kor/privacy/privacy02.jsp, KISA 해외개인정보 보호기구.

[7] 뉴시스통신사, "TUV라인란드일본지사, 'EU 개인정보 보호지침 인증 서비스' 실시", 2010. 11. 4.

[8] British Standard BS 10012: 2009, *Data protection - Specification for a personal information management system*, BSI, 2009. 5.

[9] Introducing BSI's Data Protection Online tool, http://www.bsigroup.com/en/Standards-and-Publications/Committee-Members/Committee-member-news/Winter-2009/Introducing-BSIs-Data-Protection-Online-tool-/.

[10] http://www.itlkorea.kr/newsletter/news letter_view.php?No=36&start=480.

[11] Personal Data Act(1998:204), 1998.

[12] 김성곤, "독일「연방정보보호법」의 개정 동향", 한국인터넷진흥원, 인터넷 법제동향 제28호, 2010. 1.

[13] "개인의 신용평가와 관련한 연방빙보보호법의 주요 개정 내용", 한국인터넷진흥원, 인터넷 법제동향 제31호, 2010. 4.

[14] "독일 연방의회「근로자의 개인정보보호에 관한 법률안」현재 심의중", 한국인터넷진흥원, 인터넷 법제동향 제46호, 2011. 7.

[15] 류승훈, "독일 연방정보보호법(2)", 최신 외국법제정보 2008-9, 한국법제연구원, 2008. 9.

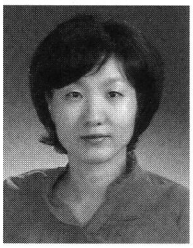
[16] 양용석, "해외 개인정보보호 법과 제도 동향", 주간기술동향 통권 1443호, pp. 17-29, 2010. 4.

[17] "佛「개인정보 보호법안」하원 검토", 한국인터넷진흥원, 인터넷 법제동향 제48호, 2011. 9.

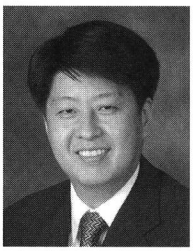
[18] The Data Protection Act, 1984.

[19] 문정욱, "영국의 국가정보화 전략 및 시사점: 'Government ICT Strategy'를 중심으로", 방송통신정책 제22권 17호, 정보통신정책연구원 2010. 9.

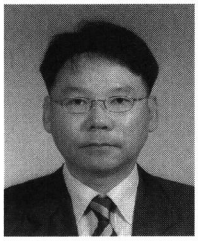
〈著者紹介〉



전 은 정 (Eun-Jung JUN)
학생회원
2006년 8월: 순천향대학교 정보보호학과 석사(공학석사)
2010년 3월~현재: 순천향대학교 정보보호학과 박사과정
<관심분야> 개인정보보호



김 학 범 (Hak-Beom KIM)
정회원
1990년 8월: 중앙대학교 대학원 전자계산학과 졸업(공학석사)
2001년 2월: 아주대학교 대학원 컴퓨터공학과 졸업(공학박사)
1991년 10월~1996년 6월: 한국전산원 주임연구원
1996년 7월~2001년 8월: 한국정보보호진흥원 기술표준팀장
2001년 9월~2003년 1월: (주)드림시큐리티 상무이사
2003년 2월~2005년 3월: (주)장미디어인터렉티브 상무이사
2008년 4월~2009년 6월: 인포섹(주) 수석컨설턴트
2009년 7월~2010년 12월: 에스지에이(주) 연구소장
2001년 3월~2009년 2월: 순천향대학교 정보보호학과 겸임교수
2005년 9월~현재: 동국대학교 국제정보대학원 겸임교수
2011년 7월~현재: 한국정보보호학회 이사
2011년 9월~현재: (주)지엔에스인증원 ISMS본부장
<관심분야> ISO 27001, 클라우드 컴퓨팅 보안, 개인정보보호



염 흥 열 (Heung-Youl YOUM)
정회원
1981년 2월: 한양대학교 전자공학과 학사 졸업
1983년 9월: 한양대학교 대학원 전자공학과 석사 졸업
1990년 2월: 한양대학교 전자공학과 박사 졸업
1982년 12월~1990년 9월: 한국전자통신연구소 선임연구원
1990년 9월~현재: 순천향대학교 정보보호학과 정교수
1997년 3월~2000년 3월: 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재: 한국정보보호학회 총무이사, 학술이사, 교육이사, 논문지편집위원 위원장, 수석부회장(역), 학회장(현)
2005년~2008년: ITU-T SG17 Q9 Rapporteur(역)
2006년 11월~2009년 2월: 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재: 국정원 암호검증위원회 위원
2009년~현재: ITU-T SG17 부의장/SG17 WP2 의장
<관심분야> 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜